НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Методика проведення комплексного аудиту системи управління інформаційної безпеки»

Виконав:
студент ІІ курсу, групи ТС-71мп
Павленко Володимир Валерійович _____

Керівник:
доктор технічних наук, професор кафедри ТС
Горицький Віктор Михайлович _____

Рецензент:

_____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2018 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Л.О. Уривський

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Павленку Володимиру Валерійовичу

1. Тема дисертації «Методика проведення комплексного аудиту системи управління інформаційної безпеки», науковий керівник дисертації Горицький Віктор Михайлович, професор кафедри ТС, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження – система управління інформаційною безпекою.

4. Предмет дослідження – комплексний аудит системи управління інформаційною безпекою

5. Перелік завдань, які потрібно розробити:

а) визначення місця аудиту СУІБ в системі забезпечення інформаційної безпеки;

б) аналіз стандартів щодо здійснення аудитів СУІБ та принципів проведення аудиту СУІБ;

в) дослідження питань оцінювання аудиторів СУІБ та їх компетентності для задоволення потреб програми аудиту СУІБ;

г) дослідження основних принципів розробки програми та цілей аудиту СУІБ;

д) аналіз провідних вказівок щодо управління програмою аудиту;

е) розрахунок тривалості аудиту СУІБ та оптимальних точок переходу між етапами аудиту.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу

Плакат №1 «Тема, мета та завдання магістерської дисертації»

Плакат №2 «Актуальність та постановка задачі»

Плакат №3 «Порівняння стандартів для побудови та аудиту СУІБ»

Плакат №4. «Динаміка росту показника якості аудиту»

Плакат №5. «Висновки»

7. Орієнтовний перелік публікацій: Міжнародна конференція "Проблеми телекомунікацій" на базі Інституту телекомунікаційних систем і НДІТ НТУУ "КПІ"., 2018. (м. Київ)

8. Дата видачі завдання – 21.10.2017

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Методи та засоби забезпечення безпеки інформаційних технологій у відповідності до міжнародних стандартів		
2	Аналіз стандартів щодо здійснення аудитів СУІБ		
3	Принципи проведення аудиту СУІБ		
4	Управління програмою аудита СУІБ		
5	Аналіз діючих національних методик проведення аудиту СУІБ		
6	Оцінювання аудиторів СУІБ та їх компетентність		
7	Розробка програми та цілей аудиту		
8	Розрахунок тривалості аудиту СУІБ та знаходжчення точок переходу між етапами аудиту		
9	Узагальнення результатів досліджень, підготовка підсумкового звіту. Подання роботи до приймання, та її захист.		

Студент Павленко В.В.

Науковий керівник дисертації Горицький В.М.

РЕФЕРАТ

Темою магістерської дисертації є дослідження методики проведення комплексного аудиту СУІБ.

Робота містить 93 сторінки, зокрема 9 ілюстрацій, 5 таблиць та 22 джерел інформації.

Тема є доволі актуальною в наш час, адже сучасний світ вимагає підвищеної уваги до питань інформаційної безпеки. Збитки організацій від різноманітних атак та несанкціонованого доступу сягає десятків мільйонів доларів. У зв'язку з цим забезпечення захисту інформації стає особливо пріоритетним завданням для успішних корпорацій, в яке вони готові вкладати дедалі більше ресурсів. Комплексний аудит СУІБ є одним з факторів успішного захисту інформації.

Таким чином, метою роботи є покращення методики проведення комплексного аудиту СУІБ шляхом знаходження рівнів показників якості, при яких варто переходити до наступного етапу аудиту.

Об’єктом дослідження є система управління інформаційною безпекою. Предметом дослідження є методика проведення комплексного аудиту системи управління інформаційною безпекою.

При виконанні роботи застосовувалася мова програмування Python із встановленим модулем matplotlib для побудови графічних зображень.

У дисертації було запропоновано методику оптимального за часом переходу з одного етапу аудиту СУІБ до іншого на основі знаходження рівнів показників якості аудиту – ймовірності запобігання несанкціонованому доступу.

Основні результати дисертаційного дослідження оприлюднено в ході Міжнародної конференції "Проблеми телекомунікацій" на базі Інституту телекомунікаційних систем і НДІТ НТУУ "КПІ"., 2018. (м. Київ)

ABSTRACT

The topic of the master thesis is to study a method of conducting complex audit of information security management system.

The work contains 93 pages, including 9 illustrations, 5 tables and 22 sources.

Theme of master's thesis is relevant because the modern world requires increased attention to information security issues. Organizations lose millions of dollars due to different attacks. Information security must have the highest priority for the successful corporations. In this regard, they are ready to invest more and more resources to make information more secure. Complex audit of ISMS is one of the factors of information security.

The purpose of the thesis is to improve a method of conducting complex audit of ISMS by finding the levels of quality scores to move to the next stage of the audit.

The object of research is an ISMS. The subject of research is a method of conducting complex audit of ISMS.

Python used for calculations and installed Python module for graphic illustrations.

The method of finding the levels of quality scores (probability of preventing unauthorized access) to move to the next stage of the audit was proposed.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ІТ	Інформаційні технології
ІТС	Інформаційно-телекомунікаційні системи
СЗІБ	Система забезпечення інформаційної безпеки
СУІБ	Система управління інформаційною безпекою
COBIT	Control Objectives for Information and Related Technologies
IEC	Міжнародна електротехнічна комісія
ISO	Міжнародна організація зі стандартизації
ITIL	IT Infrastructure Library

ВСТУП

Сучасна та ефективна система забезпечення інформаційної безпеки (СЗІБ) являє собою комплекс заходів, спрямованих на захист конфіденційної корпоративної інформації на всіх стадіях її життєвого циклу: в процесі обробки, передачі, зберігання.

Це особливо важливо для організацій з територіально розподіленою інфраструктурою, в який здійснюється безперервний обмін даними між окремими підрозділами та регіональними представництвами.

СЗІБ в повній мірі виконує свої функції, тільки якщо є ретельно спланованою, налагодженою системою, в діяльності якої використовуються передові технології та дотримуються міжнародні стандарти інформаційної безпеки. Саме такий підхід повинні здійснювати організації України при створенні, впровадженні та супроводі СЗІБ в організаціях будь-яких масштабів і сфер діяльності.

Безперервне функціонування СЗІБ відбувається завдяки поєднанню організаційних і технічних заходів, що застосовуються відповідно до управлінських рішень, які розробляються в рамках системи управління інформаційною безпекою (СУІБ).

При створенні сучасних СЗІБ розробники повинні діяти у відповідності зі стандартами, що описують основні етапи проектування та впровадження автоматизованих систем.

Таким чином, робота фахівців IT (інформаційні технології) з створення СЗІБ проходить за наступною схемою:

а) аудит функціонуючих в організації інформаційних систем, обстеження обладнання і програмних процесів, що відповідають за безпеку інформації на всіх етапах її життєвого циклу;
б) розробка СУІБ відповідно до міжнародних стандартів;
в) розробка технічного завдання на створення СЗІБ відповідно до міжнародних стандартів, кращими практиками, об'єктивними

вимогами даної сфери бізнесу, а також з урахуванням індивідуальних побажань Замовник;

г) проектування СЗІБ, що включає:
   1) оформлення робочої, експлуатаційної та кошторисної документації;
   2) розробку основних ІТ-рішень з комплексного захисту конфіденційної корпоративної інформації;
   3) створення технічного і ескізного проектів побудови СЗІБ;
   4) розробку програми і методів випробування спроектованої СЗІБ;

д) впровадження СЗІБ, в тому числі і СУІБ, в ході чого:
   1) в організацію поставляються всі необхідні програмні продукти та обладнання;
   2) виробляються монтажні роботи;
   3) організовуються попередні і приймальні (атестаційні) випробування процесів і програмно-апаратного комплексу СЗІБ;
   4) проводиться навчання персоналу компанії-замовника роботі з створеної СЗІБ;
   5) створення та впровадження СУІБ.

Таким чином, створення СЗІБ – це комплексний підхід до захисту конфіденційної корпоративної інформації із залученням кваліфікованих спеціалістів та експертів. При цьому проекти повинні (можуть) розроблятися і реалізуватися відповідно до міжнародних стандартів інформаційної безпеки, а також з урахуванням кращих світових практик та думок експертів сучасного ІТ-ринку.

Проблема створення ефективних систем управління інформаційної безпеки (СУІБ) з метою забезпечення стабільного розвитку сучасної організації та успішної протидії загрозам в умовах жорсткої конкуренції добре відома. Дану систему необхідно піддавати повноцінному аудиту на відповідність вимогам інформаційної безпеки, наприклад стандартам серії ISO 27k. [1, 2] Тому важливість проведення якісної перевірки СУІБ важко переоцінити.

Аудит СУІБ дозволяє визначити найбільш вразливі місця в захисті компанії, допомагає оцінити ефективність діючих організаційно-технічних заходів щодо захисту інформаційної системи організації [3]. Рівень забезпечення інформаційної безпеки різниться в залежності від конкретної компанії, але повинен відповідати деякому мінімальному набору вимог безпеки.

РОЗДІЛ 1. МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ШЛЯХОМ ЗДІЙСНЕННЯ АУДИТУ СУІБ

1.1 Складові та особливі властивості інформаційної безпеки

Поняття інформаційної безпеки може розглядатись як в широкому, так і в вузькому розумінні – в залежності від області його використання.

Під інформаційною безпекою в широкому розумінні розуміють стан захищеності життєво важливих інтересів людини, суспільства чи держави, при запобіганні нанесення шкоди у зв'язку неповної, невчасної та невірогідної інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. [4]

Звертаючись до інформаційного права, інформаційна безпека є однією з сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави. Також відбувається акцентування уваги на загрозах цим інтересам та на механізмах усунення чи запобігання таким загрозам правовими методами.

Залежно від виду загроз інформаційна безпека може розглядатись як забезпечення стану захищеності: особистості, суспільства, держави від впливу неякісної інформації; інформації та інформаційних ресурсів організації від неправомірного впливу сторонніх осіб; інформаційних прав і свобод людини і громадянина.

Інформаційна безпека особистості може характеризуватись як стан захищеності особистості, соціальної групи та об’єднання людей від впливів, що здатні змінювати психічні стани і психологічні характеристики людини проти їхньої волі та бажання, її поведінку та обмежувати свободу вибору.

Інформаційна безпека держави характеризується мірою захищеності держави та стійкості основних сфер життєдіяльності відносно небезпечних

інформаційних впливів, причому як з упровадження, так і добування інформації.

Інформаційна безпека організації – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонічного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства. Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають відповідні повноваження, у відповідності із законодавством. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави.

Основними завданнями такої системи є:

- виявлення і прогнозування дестабілізуючих факторів та інформаційних загроз інформаційних життєво важливим інтересам особистості, суспільства та держави;
- здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;
- створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Сутність основних понять та змісту інформаційної безпеки і системи її забезпечення приведена на рисунку 1.1.1. [5]

Рисунок 1.1.1 Основні поняття та зміст інформаційної безпеки

Забезпечення нормативно-правових основ ІБ (інформаційна безпека) виконується документами:

- Конституція України;
- закони України ("Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про Основні засади розвитку інформаційного суспільства в Україні", "Про основи національної безпеки України");

- нормативно-правові акти Президента і Кабінету Міністрів України (Стратегія національної безпеки,
- Доктрина інформаційної безпеки України, Концепція технічного захисту інформації в Україні,
- Положення про технічний захист інформації в Україні);
- міжнародні та державні стандарти, які визначають взаємовідносини між різними міністерствами, відомствами та іншими державними установами в частині забезпечення інформаційної безпеки;
- НД ТЗІ (нормативні документи системи технічного захисту інформації);
- відомчі нормативні документи в рамках їх відповідальності.

Рівні нормативно-правового забезпечення ІБ представлено на рисунку 1.1.2. [5]

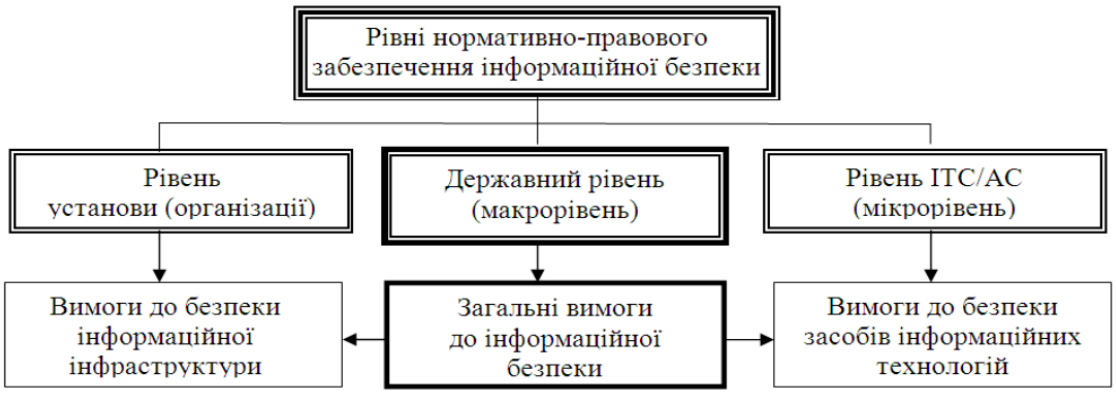

Рисунок 1.1.2 Рівні нормативно-правового забезпечення інформаційної безпеки

Основу державного рівня нормативно-правового забезпечення інформаційної безпеки складають Закони України, Укази Президента, Постанови Кабінету Міністрів України та ін., вимоги яких є обов’язковими для виконання на всіх рівнях. Згідно Закону України "Про захист інформації в ІТС" інформація, яка є власністю держави повинна оброблятися із застосуванням комплексних систем захисту інформації з підтвердженою відповідністю (за результатами державної експертизи). При проектуванні захищених

інформаційно-телекомунікаційних систем важливо чітко визначити, яким вимогам вони повинні відповідати, перелік основних показників якості, методику контролю та оцінки їх ефективності. На сьогодні, ця задача може бути вирішена за допомогою спеціально розроблених нормативних документів, які отримали назву стандартів інформаційної безпеки. В рамках стандартів міжнародного (стандарти ISO) та національного рівнів (ДСТУ, НД ТЗІ) щодо інформаційної безпеки визначаються вимоги до захисту інформації, або її властивостей.

1.2 Методи та засоби забезпечення безпеки інформаційних технологій у відповідності до міжнародних стандартів

21 вересня 2018 року аналітичний центр компанії InfoWatch представив результати глобального дослідження витоків конфіденційної інформації в першому півріччі 2018 року. Всього за досліджуваний період було зареєстровано 1039 випадків витоку конфіденційної інформації, що на 12% більше, ніж роком раніше. Зокрема, обсяг інформації, скомпрометованої з вини хакерських та інших атак під впливом зовнішнього порушника, зменшився в десять разів, склавши лише близько 0,5 мільярдів записів. При цьому в результаті порушень всередині організацій постраждали більше 1,5 мільярдів записів даних, включаючи персональні і платіжні.

Як і раніше в світі переважає мережевий канал витоків даних (70%). Через мережу найчастіше реалізуються складні умисні атаки, які завдають найбільшої шкоди для організацій. На частку контрольованих каналів передачі інформації, таких як поштові сервіси і паперові носії, припадає невеликий відсоток умисних витоків – трохи більше 10%. Випадкові витоки, для здійснення яких не потрібна спеціальна підготовка, відбуваються по різних каналах – поряд з мережевими каналами також зафіксована велика частка витоків через паперові носії, електронну пошту і при втраті або крадіжці обладнання.

У розподілі категорій по винуватцям витоків переважають рядові співробітники – 56%, в той час як на частку привілейованих користувачів – керівників і системних адміністраторів, припадає близько 4% інцидентів. Ще більше 3% витоків припало на підрядників, 38% на зовнішніх по відношенню до організації зловмисників (рисунок 1.2.1).

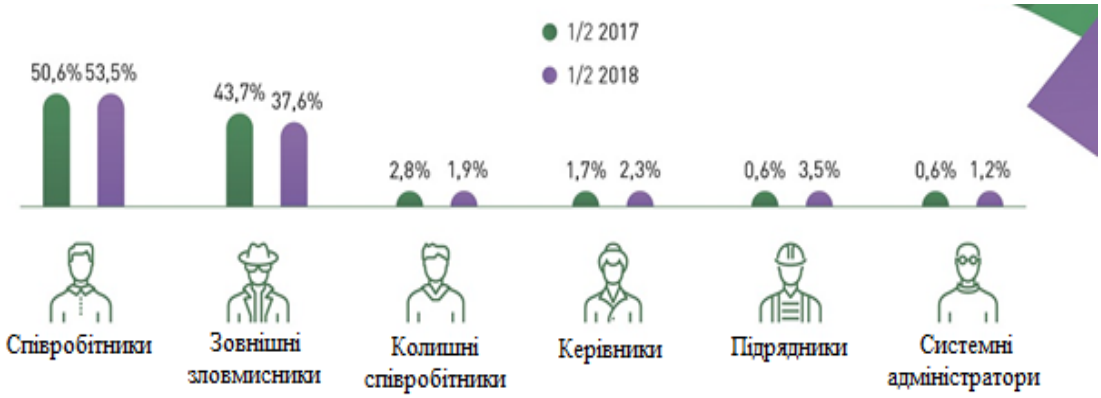

Рисунок 1.2.1 Винуватці витоків інформації

Більшу частину обсягу витоків, як і роком раніше, становить найбільш чутлива інформація – персональні і платіжні дані – 90% інцидентів (рисунок 1.2.2).

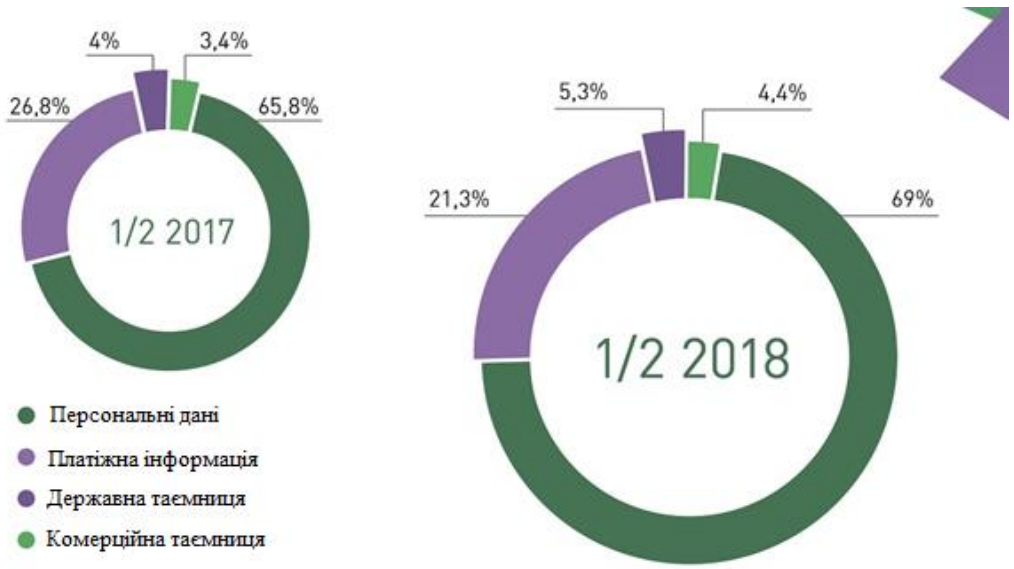

Рисунок 1.2.2 Розподіл витоків за типом інформації

Як бачимо, з розвитком інформаційних систем загрози, які виходять від співробітників організацій та зовнішніх зловмисників, давно стали дуже серйозними, а збиток від їх дій обчислюється десятками мільярдів доларів. Постійно зростає потік повідомлень про інциденти, пов'язані з порушенням своїх зобов'язань і прав авторизованими користувачами, які навмисно саботують свою компанію і передають інформацію конкурентам. Одночасно змінюється і бізнес-середовище, яке все більше покладається на аутсорсинг, підрядні компанії і сторонні технологічні платформи, що призводить до того, що цінна бізнес-інформація стає доступною все більшій кількості людей. Щоб запобігти витоку інформації потрібно забезпечити її надійний захист.

Отже, забезпечення інформаційної безпеки – сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в обробці, зберіганні та поширенні інформації.

Класифікація засобів захисту інформації:

1) Засоби захисту від несанкціонованого доступу:
   - засоби авторизації;
   - мандатне управління доступом;
   - виборче управління доступом;
   - управління доступом на основі ролей;
   - аудит.
2) Системи аналізу та моделювання інформаційних потоків.
3) Системи моніторингу мереж:
   - системи виявлення й запобігання вторгнень;
   - системи запобігання витоків конфіденційної інформації.
4) Аналізатори протоколів.
5) Антивірусні засоби.
6) Міжмережеві екрани.
7) Криптографічні засоби:
   - шифрування;
   - цифровий підпис.

8) Системи резервування:
   - резервне копіювання;
   - відмовостійкий кластер;
   - Резервний Центр Обробки Даних для катастрофостійкої інформаційної системи.
9) Системи безперебійного живлення:
   - джерела безперебійного живлення;
   - резервні лінії електроживлення;
   - генератори електроживлення.
10) Системи аутентифікації на основі:
   - паролю;
   - ключа доступу (фізичного або електронного);
   - сертифікату;
   - біометричних даних.
11) Засоби запобігання злому корпусів і крадіжок устаткування.
12) Засоби контролю та управління доступом в приміщення.
13) Інструментальні засоби аналізу систем захисту
14) Засоби захисту від побічного електромагнітного випромінювання і наведення.

Крім засобів захисту інформації існують також методи забезпечення безпеки інформації в інформаційних системах:

1) перешкода;
2) управління доступом;
3) механізми шифрування;
4) протидія атакам шкідливих програм;
5) регламентація;
6) примус;
7) спонукання. [6]

Розглянемо кожен метод забезпечення безпеки інформації детальніше.

Перешкодою вважають метод фізичного загородження шляху зловмиснику до інформації, що захищається.

Управління доступом називають методи захисту інформації шляхом регулювання використання ресурсів інформаційної системи. Дані методи повинні протистояти можливим шляхам несанкціонованого доступу до інформації.

Управління доступом включає наступні функції захисту:

1) ідентифікацію користувачів, персоналу та ресурсів системи;
2) встановлення автентичності об'єкту або суб'єкта за пред'явленим ідентифікатором;
3) перевірку відповідності дати запрошуваних ресурсів і процедур встановленому регламенту;
4) дозвіл і створення умов роботи в межах встановленого регламенту;
5) реєстрацію звернень до ресурсів, що захищаються;
6) реагування (сигналізація, відключення, затримка робіт, відмова в запиті і т.п.) при спробах несанкціонованих дій. [6]

Механізми шифрування іншими словами – це криптографічне закриття інформації від зловмисників. Дані методи захисту досить широко застосовуються при обробці та зберіганні інформації на магнітних носіях. Також цей метод використовується при передачі інформації по каналах зв'язку великої протяжності і надійним.

Протидія атакам шкідливих програм – це комплекс різноманітних заходів організаційного характеру та використання антивірусних програм. Основним завданням є виявлення фактів зараження системи; зменшення наслідків інформаційних інфекцій, локалізація або знищення вірусів; відновлення інформації в інформаційній системі.

Під регламентацією розуміють створення таких умов автоматизованої обробки, зберігання та передачі інформації при яких норми і стандарти щодо захисту виконуються в найбільшій мірі.

Примус вимагає від користувачів та персоналу інформаційної системи дотримуватися правил обробки, передачі і використання інформації, що захищається під загрозою матеріальної, адміністративної або кримінальної відповідальності.

Спонукання – це метод захисту, при якому відбувається заохочення користувачів та персоналу інформаційної системи не порушувати встановлені порядки через дотримання сформованих моральних і етичних норм.

Технічні засоби поділяються на апаратні і фізичні.

Апаратними засобами вважають пристрої, що вбудовуються безпосередньо в обчислювальну техніку. Також це можуть пристрої, які сполучаються з нею через стандартний інтерфейс.

Фізичними засобами є різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту, здійснюють захист персоналу, фінансів, інформації від несанкціонованих дій. Прикладами можуть бути: замки на дверях, решітки на вікнах, засоби сигналізації.

Програмними засобами називають спеціальні програми та програмні комплекси, що призначені для захисту інформації в інформаційній системі.

Організаційні засоби здійснюють регламентацію виробничої діяльності в інформаційній системі таким чином, що розголошення, витік і несанкціонований доступ до конфіденційної інформації істотно ускладнюється за рахунок проведення організаційних заходів.

Законодавчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила користування, обробки і передачі інформації обмеженого доступу і встановлюються міри відповідальності за порушення цих правил.

Морально-етичні засоби захисту – це різноманітні норми поведінки, що складаються в міру поширення інформаційних систем та ІТ в країні і в світі або спеціально розробляються. Морально-етичні норми можуть бути неписані (наприклад чесність) або оформлені в якийсь статут правил чи приписів. Ці

норми, як правило, не є законодавчо затвердженими, але оскільки їх недотримання призводить до падіння престижу організації, вони вважаються обов'язковими для виконання.

1.3 Висновки з розділу 1

В даному розділі описані основні методи та засоби забезпечення інформаційної безпеки. Для ефективної боротьби із зловмисниками та витоком інформації повинні забезпечуватись нормативно-правові основи ІБ, які врегульовуються певними документами. Щоб забезпечити належний рівень ІБ потрібно побудувати СУІБ, проводити її моніторинг та підтримку, що дозволить ефективно застосовувати поєднання всіх можливих засобів та методів, що описані в даному розділі. Для цього існують різноманітні стандарти.

РОЗДІЛ 2. АНАЛІЗ СТАНДАРТІВ ЩОДО ЗДІЙСНЕННЯ АУДИТІВ СУІБ

2.1 COBIT

COBIT пропонує цілісну методологію, яка покликана допомогти у вирішенні завдання керівництва і управління IT на підприємстві. Простіше кажучи, COBIT допомагає підприємствам досягти оптимальної цінності від IT, підтримуючи баланс між отриманням вигоди і оптимізацією ризиків і ресурсів.

COBIT дає можливість керувати і управляти IT в масштабах всього підприємства, як в областях функціональної відповідальності IT, так і бізнесу, а також дозволяє враховувати потреби в IT внутрішніх і зовнішніх зацікавлених сторін. Методологія COBIT універсальна і буде корисна підприємствам будь-якого масштабу і сфери діяльності: комерційним, громадським і державним. [7]

2.1.1 Історія COBIT

Історія COBIT почалася в 1996 році, в цей час ISACA (Асоціація аудиту і контролю інформаційних систем), утворена в 1969 році випустила першу версію методології оцінки IT. Подальший розвиток було в 1998 році – версія 2, в 2000-му – версія 3, в 2005-му році вийшла версія 4. У 2007 році версія 4 була доопрацьована і в 2007 році стала нести індекс 4.1. На сьогоднішній момент аудитори паралельно використовують дві версії 4.1 і 5, яка вийшла в 2012 році та вже набрала обертів в професійному середовищі.

Зараз COBIT має зв'язок з безліччю інших стандартів і кращих практик, таких як ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 38500, ISO/IEC 31000, ISO/IEC 9000, ITIL, PRINCE2 (PRojects IN Controlled Environments 2 – Проекти в контрольованих середовищах), PMBOK (Project Management Body of Knowledge – Довідник з управління проектами), CMMI (Capability Maturity Model Integration – Модель оцінки зрілості), TOGAF (The Open Group Architecture Framework – Фреймворк в області побудови корпоративної архітектури підприємства) та інші. [7]

2.1.2 Огляд COBIT

Концепція стандарту передбачає побудову механізмів управління IT виходячи з того, яка інформація необхідна для досягнення бізнес-цілей. При цьому інформація розглядається як результат використання IT ресурсів, управління якими здійснюється в рамках IT процесів. IT ресурси включають в себе додатки, інформацію (дані в будь-якій формі), інфраструктуру, персонал.

Для досягнення цілей бізнесу інформація повинна задовольняти певним критеріям, які в стандарті COBIT називають бізнес-вимогами до інформації. Виділяють наступні бізнес-вимоги до інформації або інформаційні критерії: ефективність, раціональність, конфіденційність, цілісність, доступність, відповідність нормам і надійність інформації. Механізми управління включають в себе політики, організаційні структури, процедури і регламенти. Завданням управління IT є формулювання бажаного результату або мети, які повинні бути досягнуті шляхом реалізації механізмів управління в рамках конкретного IT процесу.

Ключовими областями управління IT є:

1) Відповідність стратегії робить акцент на зв'язок між планами бізнесу та IT; виявленні, підтримки і контролі за ціннісною пропозицією IT; а також на відповідність IT та бізнес операцій.
2) Корисність являє собою реалізацію ціннісної пропозиції, контроль за тим, щоб IT забезпечували певні стратегією переваги, зосередження на оптимізації витрат і підтвердження справжньої цінності IT.
3) Управління ресурсами присвячено питанням, пов'язаним з управлінням критичними IT ресурсами, а саме, оптимізацією інвестицій та належного керівництва додатками, інформацією, інфраструктурою і персоналом. Ключові питання стосуються оптимізації знань та інфраструктури.
4) Управління ризиками вимагає обізнаності вищого керівництва в області ризиків, чіткого розуміння корпоративного підходу в їх

відношенні, відповідності вимогам прозорості щодо істотних ризиків, включення функції або системи управління ризиками в практику організації.

5) Оцінка ефективності являє собою контроль за реалізацією стратегії, результатами проектів, використанням ресурсів, ефективністю процесів і сервісним обслуговуванням. Для цього застосовуються, зокрема, системи збалансованих показників, які перетворять стратегію в послідовність дій, результати яких вимірюються іншими, в порівнянні з бухгалтерським обліком, методами.

2.1.3 COBIT Framework Модель

Концептуальне ядро стандарту COBIT 5 сформовано з 37 високорівневих процесів, згрупованих в 5 доменів (сфери діяльності):

Оцінка, задання напряму і моніторинг (EDM – Evaluate, Direct and Monitor)

Практики всіх п'яти процесів домену EDM названі і організовані одноманітно: їх в кожному процесі по три, і вони відповідають назві домену – оцінка, напрям, моніторинг; змінюється тільки об'єкт.

Процеси з другого по четвертий спільно забезпечують оцінку, напрямок і моніторинг системи управління IT за трьома основними напрямками: формування цінності, оптимізації ризиків і оптимізації використання ресурсів.

Об'єктом для першого і п'ятого процесів виступає система керівництва IT, тобто процеси EDM02 – EDM04. І перший процес забезпечує створення і підтримання практики керівництва IT, а п'ятий – формування звітності, що забезпечує прозорість цієї практики для зацікавлених осіб, в інтересах яких здійснюється керівництво.

- EDM01 Забезпечення створення та розвитку корпоративної системи управління IT
- EDM02 Забезпечення отримання вигоди

- EDM03 Забезпечення оптимізації ризиків
- EDM04 Забезпечення оптимізації ресурсів
- EDM05 Забезпечення прозорості для зацікавлених сторін [7]

Координація, планування і організація (APO – Align, Plan and Organise)

Домен APO в COBIT 5 описує процеси, необхідні для ефективного планування та організації внутрішніх і зовнішніх ресурсів IT, включаючи: стратегічне планування, планування технологій і архітектури, планування організаційної структури, планування інновацій, управління портфелем, управління інвестиціями, управління ризиками, управління взаємовідносинами та управління якістю.

- APO01 Управління підходом до управління IT
- APO02 Управління стратегією
- APO03 Управління архітектурою підприємства
- APO04 Управління інноваціями
- APO05 Управління портфелем інвестицій
- APO06 Управління бюджетом і витратами
- APO07 Управління персоналом
- APO08 Управління відносинами
- APO09 Управління угодами про послуги
- APO10 Управління підрядниками
- APO11 Управління якістю
- APO12 Управління ризиками
- APO13 Управління безпекою [7]

У методології також описується відповідність між цілями підприємства та цілями IT і наведені універсальні приклади того, яким чином ці цілі підтримують рішення стратегічних завдань з допомогою процесів IT на основі дослідження по широкому спектру галузей.

Розробка, набуття та впровадження (BAI – Build, Acquire and Implement)

Для реалізації IT стратегії потрібно ідентифікувати, розробити або придбати відповідні IT рішення, які повинні бути впроваджені і інтегровані в

бізнес-процеси, а також внести зміни в інформаційні системи. Регламентовані процеси:

- BAI01 Управління програмами і проектами
- BAI02 Управління виявленням вимог
- BAI03 Управління вибором і впровадженням рішень
- BAI04 Управління доступністю і потужністю
- BAI05 Управління забезпеченням організаційних змін
- BAI06 Управління змінами
- BAI07 Управління передачею і прийманням змін
- BAI08 Управління знаннями
- BAI09 Управління активами
- BAI10 Управління конфігураціями [7]

Відповідно до домену, автоматизовані рішення визначені для того, щоб мінімізувати витрати на придбання і впровадження рішень, досягнення цілей і завдань організації. Прикладне програмне забезпечення купується і підтримується для підтримки бізнес-операцій з відповідними автоматизованими додатками. Технологічна інфраструктура купується і підтримується для підтримки бізнесу

Надання, обслуговування і підтримка (DSS – Deliver, Service and Support)

Домен включає надання необхідних інформаційних служб, в тому числі забезпечення безпеки і безперервності бізнесу, навчання, а також обробку даних прикладними системами. Регламентовані процеси:

- DSS01 Управління експлуатацією
- DSS02 Управління запитами на обслуговування і інцидентами
- DSS03 Управління проблемами
- DSS04 Управління безперервністю
- DSS05 Управління послугами безпеки
- DSS06 Управління контролями бізнес-процесів [7]

Моніторинг, оцінка та аналіз (MEA – Monitor, Evaluate and Assess)

Якість і відповідність IT процесів вимогам контролю повинні оцінюватися на регулярній основі. Цей домен включає в себе нагляд з боку керівництва за процесами управління в організації, а також незалежний контроль з боку внутрішніх і зовнішніх аудиторів. Регламентовані процеси:

- MEA01 Моніторинг, оцінка та аналіз продуктивності та відповідності
- MEA02 Моніторинг, оцінка та аналіз системи внутрішнього контролю
- MEA03 Моніторинг, оцінка та аналіз відповідності зовнішнім вимогами [7]

Відповідно до домену моніторингу, оцінки та аналізу можна перевірити чи все зроблено в організації відповідно до встановлених правил, стандартів і процедур. Після розробки ефективного процесу моніторингу встановлюється програма внутрішнього контролю. Внутрішній контроль допомагає процесам організації бути у відповідності до чинного законодавства та нормативно-правових актів.

2.1.4 Огляд принципів COBIT 5

Принципи – це постулати, на яких будується майже весь матеріал COBIT5. Принципів п'ять, і щонайменше за чотирма з них стоять конкретні практичні інструменти (рисунок 2.1.4). Фактично принципи забезпечують мотив і можливість для різних практичних дій з керівництва та управління IT. [7]

Рисунок 2.1.4 Принципи COBIT 5

Розглянемо кожен принцип детальніше.

Принцип 1: Відповідність вимогам зацікавлених сторін.

Система керівництва та управління IT повинна підтримувати реалізацію цілей підприємства і відповідати потребам зовнішніх і внутрішніх зацікавлених сторін.

COBIT 5 пропонує розширений і доповнений каскад цілей, що демонструє декомпозицію інтересів зацікавлених сторін у назві місії підприємства, далі в цілі керівництва та управління IT на підприємстві і нарешті – в цілі окремих компонентів системи керівництва та управління IT. Також він розширений і доповнений – тому що в COBIT 4.1 подібний каскад теж був описаний, але складався з трьох рівнів:

1) бізнес-цілі;
2) цілі IT;
3) цілі процесів IT.

У COBIT 5 над цілями бізнесу додалися вимоги зацікавлених сторін, а цілі процесів доповнені цілями інших компонентів системи управління IT. Що

не менш важливо, в COBIT 5 з'явилося явне застереження: не можна сліпо копіювати ці цілі в практику конкретної компанії, слід використовувати принцип каскадування цілей і звірятися зі списками цілей, запропонованими COBIT, для перевірки власних рішень. [7]

Принцип 2: Комплексний погляд на підприємство.

Керівництво інформаційних технологій слід розглядати як невід'ємну частину керівництва підприємством в цілому. Тому COBIT описує всі функції і процеси, необхідні, щоб керувати і управляти інформаційними технологіями на підприємстві.

Спеціальних інструментів, що підтримують другий принцип, COBIT не пропонує. Проте, дотримання цього принципу визначило склад ролей для процесів, склад зацікавлених осіб, а також структуру і склад процесної моделі. Як написано на обкладинці базової книжки підходу, COBIT 5 – «методологія для бізнесу», не для відділу IT.

Це єдиний принцип COBIT 5, не підтриманий відповідним інструментом управління, тому, особливо в порівнянні з іншими чотирма, він є принципом в чистому вигляді – важливого з ідеологічної точки зору, але другорядного з прикладної. Втім, таке враження залишається тільки якщо підходити до COBIT як до набору інструментів для управління IT. Якщо ж розглядати COBIT з позиції керівництва, тобто з позиції бізнесу, він виявляється мало не основним.

Принцип 3: Застосування єдиної інтегрованої методології.

Для керівництва та управління IT зручно використовувати єдину методологію, яка об'єднала все найкраще з сучасних стандартів і зводів знань.

В COBIT використані елементи таких стандартів як ISO/IEC 38500, ISO/IEC 27002, ISO/IEC 20000, ISO/IEC 15504, NIST (The National Institute of Standards and Technology – Національний інститут стандартів і технологій США) і інших, а також склепінь знань ITIL, PMBOK, ValIT, RiskIT, SFIA (Skills Framework for the Information Age).

Такий підхід дозволяє не просто краще розуміти зв'язку рекомендацій COBIT з уже використовуваними на підприємстві підходами і стандартами, а й

дає напрямок для розвитку компетенцій при вирішенні прикладних задач організації управління IT.

Принцип 4: Забезпечення цілісності підходу.

Для ефективного керівництва та управління IT одних процесів недостатньо. Потрібні й інші компоненти.

Ці компоненти називаються в COBIT 5 "enablers", що можна перекласти як «чинники впливу». Їх сім:

1. Політики, принципи і підходи
2. Процеси
3. Оргструктура
4. Культура, етика, поведінку
5. Інформація
6. Послуги, інфраструктура і додатки
7. Люди, навички та компетенції [7]

Три останніх об'єднані поняттям «ресурси». Для кожного фактора впливу можна прочитати коротке пояснення – в єдиній структурі, що включає в себе зацікавлені сторони, цілі, життєвий цикл, практики і продукти, а також метрики.

Структура публікацій COBIT передбачає випуск так званих Enabler guides, детально описують кожен фактор впливу. Опублікована одночасно з базовою публікацією в квітні минулого року книжка "Enabling processes" – це 230 сторінок, на яких детально описані 37 процесів. Мабуть, аналогічного рівня деталізації можна очікувати і в інших публікаціях цієї групи, коли вони вийдуть у світ.

Спроби систематизувати компоненти системи управління IT робилися і раніше. Так, ITIL пропонує читачам список з 9 «сервісних активів», які об'єднують ресурси і здібності, необхідні для управління послугами IT. Однак зазвичай ці спроби закінчуються простим перерахуванням компонентів, COBIT ж містить детальну характеристику кожного і обіцяє ще більше. Якщо до складу COBIT увійдуть enabler guides за такими напрямками, як «культура,

етика, поведінка» і «люди, навички та компетенції», цінність цього зводу знань зросте багаторазово: в даний час структурованих рекомендацій з цих питань, які враховують специфіку керівництва та управління IT , практично не існує.

Принцип 5. Поділ керівництва та управління

Повинна бути визначена чітка межа між керівництвом і управлінням. Ці дві дисципліни включають в себе різні види діяльності, вимагають різних організаційних структур і служать різним цілям: керівництво забезпечує впевненість в досягненні бізнес-цілей шляхом оцінки потреб зацікавлених сторін, умов і варіантів, завдання напряму руху через пріоритизації і прийняття рішень, порівняння фактичної продуктивності, ступеня завершення і відповідності правилам з плановими значеннями; управління полягає в плануванні, побудові, виконанні та відстеження діяльності відповідно до напряму, заданим органом керівництва, для досягнення бізнес-цілей.

COBIT пропонує референтну модель системи керівництва та управління IT, що описує п'ять процесів керівництва та 32 процесу управління. Процеси управління IT в моделі згруповані в чотири домени. В цілому модель є розвитком моделі COBIT попередніх версій – деякі процеси були об'єднані, деякі перенесені в інший домен, з'явилося кілька нових процесів. Істотно перероблена рольова модель, яка використовується при розподілі відповідальності за реалізацію процесних практик. Змінено рівень деталізації опису процесів: тепер в кожному процесі виділені ключові практики, для кожної з них визначені види діяльності. Входи і виходи (документи і записи) визначені для кожної практики, а не для процесу в цілому, як було раніше. Термінологія і структура опису процесів приведені у відповідність до вимог стандарту ISO 15504.

Модель COBIT 5 дуже детальна та дуже масштабна, добре сумісна з іншими склепіннями знань, в першу чергу з ITIL. Усунуто багато помилок і нестиковок з моделлю COBIT 4.1.

2.2 ITIL

Модель ITIL (Information Technology Infrastructure Library – Бібліотека інфраструктури інформаційних технологій) – бібліотека передового досвіду в даний час фактично стала міжнародним стандартом у сфері організації і управління інформаційними технологіями.

2.2.1 Історія ITIL

Історія ITIL почалася більше 20 років тому у Великобританії. У той час Сполучене Королівство зазнавало серйозного економічного спаду, а якість IT-послуг, що надаються британському уряду різними постачальниками, було настільки низьким, що було засноване Центральне агентство з обчислювальної техніки і телекомунікацій (Central Computer and Telecommunications Agency, CCTA, в даний час називається Office of Government Commerce, OGC), що отримало від уряду цієї країни вказівку розробити принципи ефективного і рентабельного використання IT-ресурсів в міністерствах та інших державних установах і вже на їх основі формувати підхід до надання IT-послуг, що не залежить від їх постачальника.

В агентстві була створена робоча група з представників компаній-виробників, користувачів і консультантів IT-галузі. Перед учасниками групи було поставлено завдання узагальнити передовий досвід в галузі управління IT-системами. За підсумками роботи була випущена серія з сорока книг, розроблений єдиний словник термінів. У 1989 році це видання було перероблено і видано CCTA (Central Computer and Telecommunications Agency – Центральне комп'ютерне і телекомунікаційне агентство) у вигляді книги обсягом 31 томи, що отримала назву Government Information Technology Infrastructure Management Methodology (GITMM). В середині 90-х років замість назви GITMM стали використовувати назву «ITIL».

Друга версія бібліотеки ITIL була розроблена в кінці 1990-х років. Ця версія ITIL містить 7 основних та 2 додаткових книги. Ядром її є концепція Управління IT-сервісами ITSM (IT Service Management – Управління послугами IT), яка заснована на використанні базових процесів і функцій ITIL щодо організації надання послуг відділами IT як різним співробітникам компанії, так і її клієнтам.

У 2011 році вийшла нова редакція ITIL-3. У третій версії ITIL загальна концепція залишається незмінною: бібліотека як і раніше містить опис вдалих управлінських рішень та слугує інтересам і потребам бізнесу. Автори ITIL-3 оновили структуру опису процесів, в якій виділено ядро бібліотеки і додаткові (комплементарні) розділи.

Оновлене ядро ITIL-3 складають ключові поняття і методи, що використовуються в практиці управління IT інфраструктурою вже протягом тривалого часу (в тому числі, в ITIL-2). Книги ITIL-3 з додатковими розділами включають описи застосування концепцій, викладених в ядрі, з урахуванням специфіки конкретних підприємств і організацій, зокрема в банках або на підприємствах малого бізнесу. Основні публікації ITIL-3 представлені в 5 книгах, назви яких відображають життєвий цикл сервісів (послуг) IT:

- Стратегія послуг (Service Strategies)
- Проектування послуг (Service Design)
- Впровадження послуг (Service Transition)
- Експлуатація послуг (Service Operation)
- Постійне поліпшення обслуговування (Continuous Service Improvement) [8]

2.2.2 Огляд ITIL

Переваги ITIL полягають в наступному: використання передового досвіду і перевірених знань; спрямованість діяльності IT на вирішення завдань бізнесу; використання IT служби постачальниками послуг IT для бізнес-підрозділів;

регламентування діяльності угодою IT про рівень послуг; стандартизація роботи персоналу IT; спрямованість на забезпечення оптимальної якості послуг IT для споживачів; використання підходів менеджменту якості в управлінні сервісами IT; можливість підтвердження вартості сервісу IT на підставі угоди про рівень обслуговування.

Бібліотека ITIL постійно поповнюється і допрацьовується з урахуванням нового досвіду і знань, отриманих в індустрії надання послуг IT. Передові методи ITIL, що дозволяють підвищити ефективність управління інфраструктурою IT, на сьогоднішній день використовуються багатьма великими світовими компаніями.

2.2.3 Компоненти ITIL

Як зазначалось раніше, ITIL складається з п'яти основних принципів:

1) стратегія послуг;
2) проектування послуг;
3) експлуатація послуг;
4) перетворення послуг;
5) постійне поліпшення обслуговування. [8]

У кожному компоненті ITIL є безліч процесів, які пов'язані між собою і пов'язані один з одним.

Стратегія послуг

Стратегія послуги (або побудова стратегії) – це основа життєвого циклу послуги. Відповідна йому публікація позначає фундаментальність поняття сервіс-менеджменту в контексті життєвого циклу послуги. У книзі розглядаються наступні питання: розвиток ринку IT-послуг, характеристики і типи постачальників послуг, основні якості послуги і реалізація стратегії в процесі життєвого циклу. Ключовими темами також є фінансове управління, управління попитом, організаційний розвиток і стратегічні ризики.

Постачальник повинен використовувати етап планування послуги для постановки цілей, розуміння очікувань споживачів і ринку збуту. Побудова стратегії призначене в першу чергу для того, щоб постачальник послуг зміг оцінити свої можливості і вирішити, чи може він впоратися з усіма витратами і ризиками відповідно до заявленого Портфелем послуг.

Проектування послуг

Для будь-якої IT-послуги найважливішим є надання бізнесу певної вигоди або цінності. Тому при створенні послуги постачальник повинен в першу чергу враховувати мету бізнесу. Публікація "Проектування послуги" являє собою керівництво по моделювання і поліпшення послуг, а також рекомендації з управління ними на практиці.

Цей етап описує основні принципи та методи моделювання для трансформації стратегічних цілей в набір конкретних послуг з певними якостями. Процес проектування фактично є безмежним, якщо мова йде про нові послуги. Він також включає в себе питання змін і поліпшень в рамках життєвого циклу послуги, необхідних для збільшення її цінності з точки зору споживачів.

Перетворення послуг

Transition (англ.) – переміщення, перехід або зміна з одного стану (позиції, періоду, стадії, теми і т.д.) в інший. Стосовно послуги ця стадія характеризує відповідне переміщення послуги IT з однієї стадії життєвого циклу до іншої.

Відповідна публікація в бібліотеці ITIL являє собою керівництво по тому, як ефективно реалізувати вимоги, сформульовані на стадіях проектування і побудови стратегії, на етапі експлуатації з контролем ризиків, відмов і збоїв. Книга об'єднує в собі практики в зміні, поліпшенні, публікації і розгортанні послуг, а також питання управління ризиками.

Експлуатація послуг

Експлуатація послуги втілює, по суті, етап "донесення" бізнес значення послуги від постачальника до замовників. Найбільш істотним при цьому є

ефективне надання послуги та її якісний супровід. Книга описує, як можна забезпечити стабільну експлуатацію послуги поряд з можливістю внесення змін в дизайн, масштаб, межі і т.д. Організаціям надаються інструкції, методи і інструменти для реалізації двох методів контролю – превентивного і проактивного.

Запропонована в книзі інформація може бути корисна для прийняття рішень в питаннях управління доступністю послуги, контролю попиту на послугу, оптимізації навантаження і рішення поточних проблем. Всі описані в книзі способи враховують можливості нових моделей та архітектур, таких як розподілені сервіси, обчислення за схемою "комунальна послуга" (utility computing), веб-сервіси та електронна комерція.

До слова, utility computing або надання обчислювальних ресурсів за схемою "комунальна послуга" – це бізнес-модель, коли постачальник послуг отримує гроші за фактом використання послуги, наприклад, за часом її використання. В традиційній бізнес-моделі користувач платить за володіння системою (сервісом). Провайдер таких послуг може оптимізувати використання своїх ресурсів, враховуючи різні потреби споживачів. Тут проглядається явна аналогія з наданням і використанням електроенергії, газу та більшості інших комунальних послуг, звідси і походження терміну.

Безперервне поліпшення послуги

Безперервне поліпшення послуги полягає в описі методів і засобів по збільшенню цінності послуги шляхом реалізації покращень на різних етапах життєвого циклу. Цей етап об'єднує в собі принципи, практики і методи управління якістю, змінами і покращеннями продуктивності. З публікації організації можна отримати рекомендації про те, як поступово вводити великомасштабні покращення в якість послуг, ефективність експлуатації та безперервність надання послуг. Керівництво призначене для забезпечення зворотного зв'язку результатів покращень з етапами планування, моделювання та перетворення. Крім цілей споживачів, послуга повинна відображати також стратегію і політику постачальника послуг.

2.3 ISO/IEC 27001

Стандарт ISO/IEC 27001 містить керівництво як по впровадженню СУІБ, так і по отриманню сертифіката третьої сторони, що свідчить про те, що засоби управління безпеки існують і функціонують відповідно до вимог цього стандарту. Стандарт ISO/IEC 27001 описує СУІБ як всеохоплюючу систему менеджменту, побудовану на принципах бізнес-ризиків для впровадження, експлуатації, моніторингу та підтримки системи управління безпекою. СУІБ повинна охоплювати всі аспекти організаційної структури, політик, планованих дій, практик, процедур, процесів і ресурсів.

2.3.1 Історія ISO/IEC 27001

В 1992 році Міністерство торгівлі і промисловості Великобританії опублікувало Кодекс управління інформаційною безпекою (Code of Practice for Information Security Management). Даний документ ліг в основу міжнародного стандарту, яким будуть слідувати тисячі організацій по всьому світу.

В 1995 році Британський інститут стандартів (BSI) прийняв Кодекс управління інформаційною безпекою в якості національного стандарту Великобританії і зареєстрував його під номером BS 7799 – Part 1.

В 1998 році BSI публікує стандарт BS7799-2, що складається з двох частин, одна з яких включила в себе звід практичних правил, а інша – вимоги до систем менеджменту інформаційної безпеки. У стандарті була представлена процедура вдосконалення заходів забезпечення інформаційної безпеки, відповідно до циклу Демінга (Plan (плануй) – Do (виконуй) – Check (перевіряй) – Act (дій)), а також системний підхід до управління заходами.

В процесі таких переглядів перша частина була опублікована як BS 7799: 1999, Частина 1. В 1999 році ця версія стандарту була перероблена і передана в Міжнародну Організацію по Сертифікації.

В 2000 році затверджений в якості міжнародного стандарту ISO/IEC 17799: 2000 (BS 7799-1: 2000). Останньою версією даного стандарту, прийнятої в 2005 році, є ISO/IEC 17799: 2005.

У вересні 2002 року в силу вступила друга частина стандарту BS 7799 Part 2 Information Security management – specification for information security management systems (Специфікація системи управління інформаційною безпекою).

В 2005 році стандарт ISO/IEC 17799 був включений в лінійку стандартів 27-й серії і отримав новий номер – ISO/IEC 27002: 2005.

25 вересня 2013 року було опубліковано оновлений стандарт ISO/IEC 27001 до: 2013 «Системи Менеджменту Інформаційної Безпеки. Вимоги »(Information security management systems – Requirements). Зміни торкнулися як структури стандарту, так і вимог. [9]

Історія стандарту ISO/IEC 27001 зображена на рисунку 2.3.1.

Рисунок 2.3.1 Історія розвитку ISO/IEC 27001

2.3.2 Огляд ISO/IEC 27001

Однією з причин подібного поновлення з 2005 до 2013 року можна відзначити появу Додатку SL (AnnexSL) першої частини директив ISO, що уніфікує численні стандарти на системи менеджменту і визначає для них нову

єдину високорівневу структуру. Зміни в порівнянні із стандартом 2005 року відображені в таблиці 2.3.2.1.

Таблиця 2.3.2.1 – Порівняння розділів

ISO/IEC 27001:2005	ISO/IEC 27001:2013
0. Введення 1. Область застосування 2. Нормативні посилання 3. Терміни та визначення 4. Система інформаційної безпеки (50) 5. Зобов'язання керівництва (18) 6. Внутрішні аудити (4) 7. Аналіз системи менеджменту (16) 8. Удосконалення (14)	0. Введення 1. Область застосування 2. Нормативні посилання 3. Терміни та визначення 4. Контекст організації (8) 5. Лідерство (19) 6. Планування (39) 7. Підтримка (28) 8. Операції (Експлуатація) (9) 9. Оцінка (Вимірювання) результативності (29) 10. Удосконалення (Поліпшення) (16)
102	148

Як помітно з таблиці, при порівнянні стандартів ISO/IEC версії 2013 року із версією 2005 кількість обов'язкових контрольних точок розділів стандарту зросла з 102 до 148. Зросла і кількість самих розділів.

Кількість засобів управління у Додатку А зменшилася з 133 до 114 (таблиця 2.3.2.2), але це зовсім не означає, що впровадження стандарту стало простіше, оскільки деякі вимоги, які були менш важливі, вимагають тепер більшої уваги та впливу.

Таблиця 2.3.2.2 – Порівняння засобів управління

ISO/IEC 27001:2005	ISO/IEC 27001:2013
A.5 Політика в області безпеки (2) A.6 Організація системи безпеки (11) A.7 Класифікація активів і управління (5) A.8 Безпека і персонал (9) A.9 Фізична і зовнішня безпека (13) A.10 Менеджмент комп'ютерів і мереж (32) A.11 Управління доступом до системі (25) A.12 Придбання, розробка та обслуговування інформаційних систем (16) A.13 Менеджмент інцидентів (5) A.14 Забезпечення безперервності бізнесу (5) A.15 Відповідність законодавству (10)	A.5 Політики інформаційної безпеки (2) A.6 Організація інформаційної безпеки (7) A.7 Безпека людських ресурсів (персоналу) (6) A.8 Управління активами (10) A.9 Управління доступом (14) A.10 Криптографія (2) A.11 Фізична безпека і захист від навколишнього середовища (15) A.12 Безпека операцій (14) A.13 Безпека комунікацій (7) A.14 Придбання, розробка та обслуговування інформаційних систем (13) A.15 Взаємовідносини з постачальниками (5) A.16 Менеджмент інцидентів (7) A.17 Забезпечення безперервності бізнесу (4) A.18 Відповідність законодавству (8)
133	114

Всі поповнення-зміни в стандарті ISO/IEC 27001: 2013 підкреслюють зростаючу важливість систем менеджменту і необхідність приділяти більше уваги менеджменту інформаційної безпеки.

Структура стандарту дозволяє вибрати ті засоби управління, які мають відношення до конкретної організації або сфери відповідальності всередині організації. У зв'язку з цим, виділяється ряд ключових елементів управління, що подаються як фундаментальні. При цьому, поряд з елементами управління для комп'ютерів та комп'ютерних мереж, стандарт приділяє велику увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам.

Безумовно, що не всі пункти стандарту можливо застосовувати в умовах кожної організації, тому в стандарті реалізовано підхід, при якому його використовують як деяке "меню", з якого слід вибирати елементи, для конкретних умов. Цей вибір здійснюється на основі оцінки ризику та ретельно обґрунтовується.

2.3.3 Принципи ISO/IEC 27001

Стандартом ISO/IEC 27001: 2005 на основі процесного підходу стосовно менеджменту ІБ реалізовувалася циклічна модель управління якістю PDCA (Plan – Do – Check – Act) представлена на малюнку 2.3.3.

Перше, що може відразу кинутися в очі при розгляді ISO/IEC 27001:2013 – відсутність явного відображення представленої у версії 2005 р моделі PDCA. Однак при уважному аналізі структури нового документа можна побачити, що цикл PDCA в ньому все ж простежується – в структурі виділяються розділи, розташовані послідовно один за іншим:

- Планування (Planning);
- Виробнича діяльність (Operation);
- Оцінка ефективності (Performance evaluation);
- Покращення (Improvement).

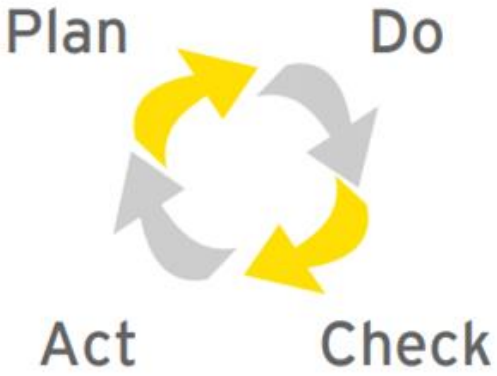

Рисунок 2.3.3 Цикл PDCA

Відповідно до моделі PDCA побудова СУІБ починається з етапу «Планування», в якому проводиться оцінка стану ІБ з урахуванням загроз і вразливостей, пов'язаних з інформаційними активами організації. Проводиться вибір необхідних заходів і засобів контролю та управління ІБ, визначаються цілі їх застосування, а також цілі застосування заходів і засобів контролю та управління для обробки ризиків. Розробляються і реалізуються політики і процедури, що повинні охоплювати наступні ключові процеси:

- управління активами;
- управління ризиками;
- управління заходами контролю;
- управління персоналом;
- управління документацією та записами СУІБ;
- управління інцидентами;
- управління ефективністю системи;
- управління змінами (перегляд і модернізація системи);
- управління безперервністю бізнесу і відновлення після переривань. [10]

На етапі «Впровадження» проводиться впровадження обраних заходів і засобів управління і контролю для досягнення цілей ІБ, визначається спосіб вимірювання результативності СУІБ, проводяться вимірювання заходів і засобів управління і контролю. Основні пункти реалізації етапу:

1) формулювання і впровадження плану обробки ризиків;
2) впровадження обраних контролів;
3) проведення навчання співробітників;
4) управління функціонуванням СУІБ;
5) надання необхідних ресурсів СУІБ.

На етапі «Перевірка» здійснюється аналіз результативності СУІБ, проводиться перегляд оцінки ризиків, з урахуванням результативності СУІБ, проводиться підтвердження ефективності СУІБ з урахуванням результатів попередніх аудитів, визначаються напрямки вдосконалення СУІБ, формуються вихідні дані для прийняття рішення щодо вдосконалення СУІБ, розвитку способів оцінювання результативності заходів і засобів управління і контролю. Основні пункти реалізації етапу:

1) виконання процедур моніторингу;
2) перегляд і оцінка ефективності СУІБ;
3) проведення внутрішніх аудитів СУІБ;
4) оновлення плану заходів по вдосконаленню СУІБ;
5) збереження записів про інциденти інформаційної безпеки .

На останньому етапі «Дія» проводиться реалізація прийнятих рішень щодо підтримки та поліпшення СУІБ:

1) впровадження визначених вдосконалень;
2) впровадження корегувальних та запобіжних заходів;
3) інформування щодо визначених вдосконалень та заходів.

2.3.4 Сімейство стандартів ISO/IEC 27000

Взагалі перелік стандартів серії ISO/IEC 27000 включає близько 60-ти найменувань – від стандарту ISO/IEC 27001 до стандарту ISO/IEC 27799. Деякі з них знаходяться в стані розробки, а інші вже повноцінно функціонують. Найбільш значимі з них приведені в таблиці 2.3.4. [11]

Таблиця 2.3.4 – Основні стандарти ISO/IEC 27000

Стандарт	Рік випуску	Назва
ISO/IEC 27000	2018	Управління ІБ. Короткий огляд і словник
ISO/IEC 27001	2013	СУІБ. Вимоги
ISO/IEC 27002	2013	Звід практики для управління ІБ
ISO/IEC 27003	2017	Керівництво по реалізації СУІБ
ISO/IEC 27004	2016	Вимірювання в управлінні ІБ
ISO/IEC 27005	2011	Ризик-менеджмент ІБ
ISO/IEC 27006	2015	Вимоги до органів аудиту і сертифікації СУІБ
ISO/IEC 27007	2017	Настанови щодо аудиту СУІБ
ISO/IEC 27011	2016	Настанови щодо управління ІБ для телекомунікацій

Сімейство стандартів СУІБ складається містить кілька важливих структурних компонентів. Ці компоненти відображені в нормативних стандартах, що встановлюють вимоги до СУІБ (ISO/IEC 27001) і вимоги до органів з сертифікації (ISO/IEC 27006), які здійснюють сертифікацію на відповідність ISO/IEC 27001, а також додаткові вимоги, пов'язані з впровадженням СУІБ в конкретних галузях (ISO/IEC 27009). Інші стандарти містять рекомендації з різних аспектів впровадження СУІБ, описуючи загальний процес, а також рекомендації для конкретних галузей.

Кожен із стандартів сімейства віднесений до певного типу (ролі) в рамках сімейства і вказано його номер документу. Діюча класифікація (на прикладі основних стандартів):

1) стандарти, що описують загальні принципи і термінологію:
    - 27000
2) стандарти, що встановлюють вимоги:
    - 27001
    - 27006
3) стандарти, що містять загальні рекомендації:

- 27002
- 27003
- 27004
- 27005
- 27007

4) стандарти, в яких викладено рекомендації для спеціальних областей:
    - 27011

Розглянемо кожен із стандартів більш детально.

Стандарти, що описують загальні принципи і термінологію

ISO/IEC 27000 (справжній Міжнародний Стандарт) Інформаційна технологія – Методи і засоби забезпечення безпеки – Системи менеджменту інформаційної безпеки – Загальний огляд і термінологія [12]

Область застосування: Справжній Міжнародний Стандарт пропонує організаціям:

1) огляд сімейства стандартів на СУІБ;
2) введення в системи менеджменту інформаційної безпеки; і
3) терміни та визначення, що використовуються в усіх стандартах сімейства.

Призначення: ISO/IEC 27000 описує основи систем менеджменту інформаційної безпеки, які становлять предмет сімейства стандартів, а також визначає відповідні терміни.

Стандарти, що встановлюють вимоги

ISO/IEC 27001 Методи і засоби забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги [13]

Область застосування: Міжнародний стандарт встановлює вимоги до розробки, впровадження , функціонуванню, моніторингу, аналізу, забезпечення і поліпшення формалізованої СУІБ в контексті всіх бізнес-ризиків організації. Він встановлює вимоги до застосування засобів управління інформаційною безпекою, адаптованих під потреби кожної організації або якихось її частин.

Міжнародний стандарт може бути використаний усіма організаціями незалежно від типу, розміру і характеру бізнесу.

Призначення: ISO/IEC 27001 містить нормативні вимоги до розробки та функціонування СУІБ, включаючи набір засобів для управління ризиками та їх зниження, пов'язаних з інформаційними активами, які організація хотіла б захистити застосуванням СУІБ. Організації, що впровадили СУІБ, можуть підтверджувати її відповідність аудитами та сертифікацією. В рамках даного процесу повинні бути обрані відповідні завдання і засоби управління з Додатку А цього стандарту, щоб охопити обрані вимоги. Завдання управління і засоби управління, наведені в таблиці А.1 стандарту ISO/IEC 27001 взяті безпосередньо і повністю відповідають тим, що наведені в розділах 5 – 18 ISO/IEC 27002.

ISO/IEC 27006 Інформаційна технологія – Методи і засоби забезпечення безпеки – вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки [14]

Область застосування: Міжнародний стандарт встановлює вимоги – на додаток до вимог, що містяться в ISO/IEC 17021 – і дає рекомендації органам, які проводять аудити і сертифікацію СУІБ на відповідність ISO/IEC 27001. Він, в першу чергу, призначений для забезпечення акредитації органів сертифікації, які проводять сертифікацію на відповідність ISO/IEC 27001.

Призначення: ISO/IEC 27006 доповнює ISO/IEC 17021 в частині вимог щодо акредитації органів сертифікації, дозволяючи, таким чином, цим організаціям видавати сертифікати відповідності вимогам, встановленим в ISO/IEC 27001.

Стандарти, що містять загальні рекомендації

ISO/IEC 27002 Інформаційна технологія – Методи і засоби забезпечення безпеки – Звід норм і правил менеджменту інформаційної безпеки [15]

Область застосування: Міжнародний стандарт містить перелік загальноприйнятих завдань управління і визнаних кращих засобів управління,

які повинні використовуватися як керівництво щодо застосування при виборі та впровадженні засобів управління для забезпечення інформаційної безпеки.

Призначення: ISO/IEC 27002 містить рекомендації щодо впровадження засобів управління інформаційною безпекою. Саме розділи з 5 по 18 дають відповідні рекомендації щодо впровадження та кращим практикам для підтримки засобів управління, зазначених в розділах A.5 – A.18 ISO/IEC 27001.

ISO/IEC 27003 Інформаційна технологія – Методи і засоби забезпечення безпеки – системи менеджменту інформаційної безпеки – Керівництво по реалізації системи менеджменту інформаційної безпеки [16]

Область застосування: Міжнародний стандарт містить практичні рекомендації по впровадженню і додаткову інформацію по розробці, впровадженню, функціонуванню, моніторингу, аналізу, забезпечення і поліпшення СУІБ відповідно до ISO/IEC 27001.

Призначення: ISO/IEC 27003 пропонує процесно-орієнтований підхід до успішного впровадження СУІБ відповідно до ISO/IEC 27001.

ISO/IEC 27004 Інформаційна технологія – Методи і засоби забезпечення безпеки – Менеджмент інформаційної безпеки – Вимірювання [17]

Область застосування: Міжнародний стандарт дає рекомендації з розробки використання вимірювань для оцінки результативності СУІБ, виконання завдань управління і застосовуваних для впровадження та управління інформаційною безпекою засобів управління, встановлених в ISO/IEC 27001.

Призначення: ISO/IEC 27004 пропонує систему вимірювань, що дозволяє оцінити результативність СУІБ, яка повинна вимірюватися відповідно ISO/IEC 27001.

ISO/IEC 27005 Інформаційна технологія – Методи і засоби забезпечення безпеки – Менеджмент ризику інформаційної безпеки [18]

Область застосування: Міжнародний стандарт містить рекомендації по менеджменту ризиків інформаційної безпеки. Підхід, прийнятий в цьому

стандарті, забезпечує реалізацію загальної концепції, представленої в ISO/IEC 27001.

Призначення: ISO/IEC 27005 служить керівництвом по впровадженню процесно-орієнтованого підходу до менеджменту ризику, щоб допомогти в реалізації і виконання вимог до менеджменту ризиків інформаційної безпеки, встановлених в ISO/IEC 27001.

ISO/IEC 27007 Інформаційна технологія – Методи і засоби забезпечення безпеки – Керівництва по аудиту систем менеджменту інформаційної безпеки [1]

Область застосування: Міжнародний стандарт містить рекомендації з проведення аудитів СУІБ, а також керівництво по забезпечення компетентності аудиторів систем менеджменту інформаційної безпеки на додаток до вказівок, що містяться в ISO 19011, які застосовні до систем менеджменту в цілому.

Призначення: ISO/IEC 27007 містить рекомендації організаціям, яким необхідно проводити внутрішні або зовнішні аудити СУІБ або керувати програмою аудиту СУІБ відповідно до вимог, встановлених в ISO/IEC 27001.

Стандарти, що містять рекомендації для спеціальних областей

ISO/IEC 27011 Інформаційна технологія – Методи і засоби забезпечення безпеки – Керівництва по менеджменту інформаційної безпеки для телекомунікаційних організацій на основі ISO/IEC 27002 [19]

Область застосування: Міжнародний стандарт дає рекомендації, що забезпечують впровадження менеджменту інформаційної безпеки в телекомунікаційних компаніях.

Призначення: ISO/IEC 27011 дозволяє телекомунікаційним організаціям задовольняти базові вимоги щодо менеджменту інформаційної безпеки щодо конфіденційності, цілісності, можливості застосування і інших важливих аспектів безпеки.

2.4 Висновки з розділу 2

Вищезгадані стандарти COBIT, ITIL та ISO 27001 є найбільш широко прийнятими та найбільш часто використовуваними стандартами у всьому світі. Однак вони можуть не завжди бути сумісним з структурами всіх організацій з різноманітних причин.

В той час як в ISO 27001 поглиблено пояснюються усі аспекти інформаційної безпеки, стандарти COBIT та ITIL розглядають багато процесів інформаційних технологій з широкої точки зору. Тобто вони не є настільки ж всеосяжними, як стандарт ISO/IEC 27001 з точки зору інформаційної безпеки.

Отож, який з вищезазначених стандартів слід застосовувати для забезпечення інформаційної безпеки? Це складне питання, і воно не має очевидної відповіді. Його відповідь відрізняється відповідно до стратегій, вимог та політик компанії. Незважаючи на те, що є багато моментів, що відрізняють ці стандарти один від одного, вони мають багато спільного, особливо в галузі інформаційної безпеки.

Інші фактори, що впливають на вибір, – це бюджет та органи влади. Практики COBIT зазвичай реалізуються за рахунок коштів, отриманих від бюджету аудиту, тоді як практика ITIL та ISO/IEC 27001 зазвичай використовують бюджет IT. Тому політика управління визначатиме стандарт якому стандарту повинен бути наданий найвищий пріорітет.

Інше питання стосовно цих стандартів стосується того, який стандарт можна реалізувати легше, ніж інші. Впровадження практик ITIL набагато простіше, ніж процеси COBIT та ISO/IEC 27001, оскільки практика ITIL може бути легко впроваджена окремо в різний час, тоді як часткові реалізації стандартів COBIT та ISO/IEC є складними.

Отже, опираючись на вищезгадані фактори порівняння можна зробити висновок, що для побудови СУІБ, а отже й для проведення аудиту СУІБ найкращим стандартом є ISO/IEC 27001, що є найбільш популярним у всьому

світі та більш всеосяжний з точки зору інформаційної безпеки, ніж інші стандарти (рисунок 2.4).

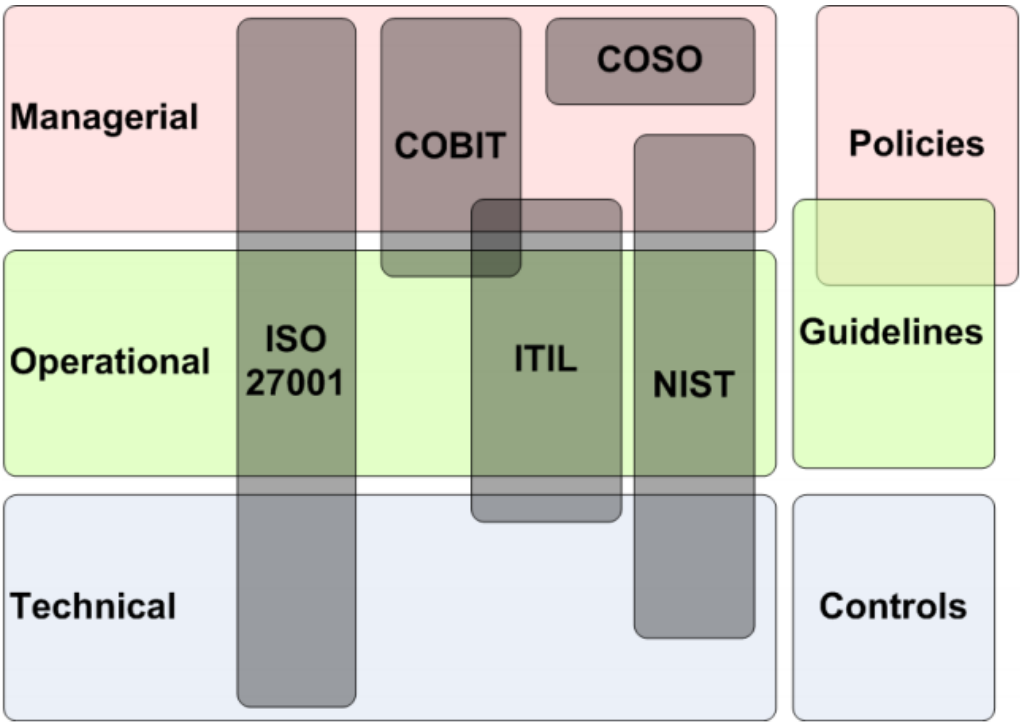

Рисунок 2.4 Порівняння стандартів

РОЗДІЛ 3. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ШЛЯХОМ ЗДІЙСНЕННЯ АУДИТУ СУІБ

3.1 Аудит СУІБ

Для того, щоб оцінити реальний стан захищеності ресурсів ІТС та її здатність протистояти зовнішнім і внутрішнім загрозам безпеці, необхідно регулярно проводити аудит інформаційної безпеки.

Системний процес отримання об'єктивних якісних і кількісних оцінок поточного стану корпоративної ІТС відповідно до критеріїв інформаційної безпеки є аудитом інформаційної безпеки.

Аудит інформаційної безпеки – це комплекс заходів, спрямованих на аналіз працездатності та відмовостійкості систем, що відповідають за захист стратегічно важливих для організації відомостей. Результатом такого аудиту повинен стати не тільки перелік вразливих місць, де існує ризик витоку конфіденційної інформації, а й розробка конкретних рекомендацій щодо усунення вже існуючих недоліків, профілактики їх виникнення в майбутньому і розвитку СУІБ в цілому.

Мета проведення аудиту інформаційної безпеки – оцінка стану безпеки ІТС та розробка рекомендацій щодо застосування комплексу організаційних заходів та програмно - технічних засобів, спрямованих на забезпечення захисту інформаційних та інших ресурсів ІТС від загроз інформаційній безпеці.

В ході аудиту інформаційної безпеки одним з завдань, які вирішуються, є аудит СУІБ, а також вирішуються наступні завдання:

1. Досліджується механізм функціонування СУІБ в організації Замовника. При необхідності на основі отриманих даних розробляються ІТ-рішення щодо підвищення працездатності і відмовостійкості цього елемента ІТ-інфраструктури.

2. Проводиться планування майбутніх вкладень в розвиток СУІБ, обґрунтування і оптимізація цих інвестицій.

3. Оцінюється відповідність наявної в організації СУІБ конкретним вимогам бізнесу.

4. Проводиться аудит СУІБ.

Як правило повний комплекс послуг з проведення аудиту інформаційної безпеки в організаціях будь-яких сфер діяльності і масштабів надають акредитовані органи з оцінки відповідності.

Керівництво з менеджменту програми аудиту СУІБ та проведення внутрішніх й зовнішніх аудитів на відповідність стандарту ISO/IEC 27001, а також керівництво з питання компетентності та оцінки аудиторів СУІБ, містить стандарт ISO/IEC 27007.

3.2 Принципи проведення аудиту СУІБ

Аудит ґрунтується на ряді принципів. Ці принципи повинні допомогти зробити аудит результативним і надійним інструментом підтримки політик керівництва і засобів управління, надаючи інформацію, яку організація може задіяти в цілях поліпшення результатів її діяльності. Дотримання цих принципів є необхідною умовою для формування значущих і достатніх висновків аудиту та дозволяє аудиторам, які працюють незалежно один від одного, робити схожі укладення в аналогічних обставинах. [20]

Настанови засновані на семи принципах:

1) Бездоганність: основа професіоналізму

Аудиторам і особам, які управляють програмою аудиту рекомендується:

- виконувати свою роботу з дотриманням етичних норм, чесно і відповідально;
- робити на аудиті тільки те, в чому компетентний;
- виконувати свою роботу неупереджено, тобто залишатися справедливим і неупередженим у всіх своїх діях;
- реагувати на будь-які втручання, які можуть вплинути на їх судження в ході аудиту.

2) Об'єктивне уявлення: зобов'язання надавати правдивий і точний звіт

Висновки, укладання аудиту і звіти з аудиту повинні точно і правдиво відображати хід аудиту.

Істотні труднощі, що зустрілися під час аудиту чи якісь розбіжності в думках між групою з аудиту та об'єктом аудиту повинні бути зафіксовані. Обмін інформацією повинен бути правдивим, точним, об'єктивним, своєчасним, ясним і повним.

3) Належна професійна старанність: старанність і розсудливість в ході аудиту

Аудиторам слід проявляти належну старанність відповідно до важливості завдання, яку вони виконують, і довірою, наданою їм замовником аудиту та іншими зацікавленими сторонами.

Важливим фактором при виконанні їх роботи з належною професійною ретельністю є здатність приймати обґрунтовані рішення в будь-яких ситуаціях, що виникають в ході проведення аудиту.

4) Конфіденційність: нерозголошення інформації

Аудиторам варто проявляти обачність у використанні і захисті інформації, отриманої в ході виконання своїх обов'язків. Інформація щодо аудиту не повинна використовуватися аудитором або замовником аудиту неналежним чином для отримання особистої вигоди або для нанесення збитку законним інтересам аудиту. Це положення відноситься і до належного поводження з особливо важливою і конфіденційною інформацією.

5) Незалежність: основа неупередженості аудиту та об'єктивності висновків аудиту

Аудитори повинні бути незалежними і у всіх випадках діяти таким чином, щоб бути вільними від упередженості і конфлікту інтересів. У разі внутрішніх аудитів аудитори повинні бути незалежні від функцій, що перевіряються, там де це можливо. Аудитори повинні зберігати об'єктивність протягом всього процесу аудиту, щоб гарантувати, що виявлені факти та висновки аудиту засновані тільки на свідченнях аудиту. [21]

У малих організаціях не завжди можна забезпечити повну незалежність внутрішніх аудиторів по відношенню до діяльності, що перевіряється, але повинно бути докладено всіх зусиль, щоб виключити упередженість і підтримувати об'єктивність.

6) Підхід, заснований на свідченнях: раціональний метод отримання надійних і відтворюваних висновків аудиту в ході систематичного процесу аудиту повинні бути перевірені. Як правило, вони засновані на вибірках з наявною інформацією, оскільки аудит проводиться в обмежений час і з обмеженими ресурсами. Слід застосовувати відповідні методи формування вибірки, тому що це тісно пов'язано з рівнем довіри до висновків аудиту.

7) Ризик-орієнтований підхід: підхід до аудиту, при якому розглядаються ризики та можливості

Ризик-орієнтований підхід повинен робити істотний вплив на планування, проведення аудитів та звітність з метою гарантії того, що аудити були зосереджені на питаннях, важливих для замовника аудиту і для досягнення цілей програми аудиту.

3.3 Висновки до розділу 3

Для забезпечення ефективної роботи системи необхідно проводити аудит СУІБ, що в свою чергу ґрунтується на ряді принципів. Тільки дотримуючись їх можна досягти формування значущих і достатніх висновків аудиту. Щоб правильно провести аудит СУІБ необхідно запросити компетентного та досвідченого аудитора. Як визначити компетентність та оцінити аудитора розглянемо в наступному розділі.

РОЗДІЛ 4. ОЦІНЮВАННЯ АУДИТОРІВ СУІБ ТА ЇХ КОМПЕТЕНТНІСТЬ

4.1 Встановлення вимог до компетентності аудиторів

Довіра до процесу аудиту і здатність досягати поставлених цілей залежить від компетентності тих осіб, які беруть участь в проведенні аудитів, в тому числі аудиторів і керівників груп з аудиту. Компетентність необхідно регулярно оцінювати за допомогою процесу, який розглядає особисті якості і здатність застосовувати знання та навички, набуті внаслідок освіти, досвіду роботи, підготовки в якості аудитора та досвіду проведення аудитів. Цей процес повинен враховувати потреби, що випливають з програми аудиту, і її цілі.

Основні вимоги, що описані в ISO/IEC 27007 в основному спираються на стандарт ISO/IEC 19011 ("Настанови щодо здійснення аудитів систем управління"). Вони є загальними для аудиторів усіх систем менеджменту, незалежно від об'єкта управління; інші є специфічними для конкретних видів систем менеджменту. Немає необхідності кожному аудитору в групі мати однакову компетентність. Однак, загальна компетентність групи з аудиту повинна бути достатньою для досягнення цілей аудиту.

Згідно ISO/IEC 27007 оцінка компетентності аудиторів повинна плануватися, здійснюватися і документуватися, щоб забезпечити об'єктивний, несуперечливий, неупереджений і надійний результат. Процес оцінки повинен включати в себе наступні чотири основні етапи:

1) визначення необхідної компетентності для задоволення потреб, що випливають з програми аудиту;
2) встановлення критеріїв оцінки;
3) вибір відповідного методу оцінки;
4) проведення оцінки.

Результати процесу оцінки повинні служити основою для:

1) вибору членів групи з аудиту;

2) визначення необхідності підвищення компетентності (наприклад, додаткова підготовка);
3) постійної оцінки результативності аудиторів.

Аудитори повинні формувати, підтримувати і підвищувати свою компетентність шляхом постійного професійного розвитку та регулярної участі в аудитах.

Визначення компетентності аудитора

При прийнятті рішення про необхідні для аудиту знаннях і навичках аудитора, що відносяться до нижчеперелічених, слід враховувати:

1) розмір, характер, складність, продукти, послуги та процеси аудиту;
2) методи аудиту;
3) вид системи менеджменту, що підлягає аудиту;
4) складність і процеси системи менеджменту, що підлягають аудиту;
5) типи та рівні ризиків і можливостей, що оброблюються системою менеджменту;
6) цілі та обсяг програми аудиту;
7) невизначеність в досягненні цілей аудиту;
8) інші вимоги, наприклад, ті, що встановлюються замовником аудиту або іншими відповідними зацікавленими сторонами, в залежності від ситуації. [22]

Особисті якості аудитора

Аудитори повинні володіти необхідними якостями, що забезпечують їм можливість діяти відповідно до принципів аудиту. Аудитори повинні проявляти професійні якості при виконанні аудиту. Згідно ISO/IEC 27007 бажана професійна поведінка передбачає, що аудитор повинен бути:

1) етичним, тобто справедливим, правдивим, щирим, чесним і стриманим;
2) відкритим, тобто мати бажання розглядати альтернативні ідеї або точки зору;
3) дипломатичним, тобто тактовним у спілкуванні з людьми;

4) наглядовою, тобто активно відслідковувати навколишнє оточення і дії;
5) проникливим, тобто знати і бути в змозі зрозуміти ситуацію;
6) гнучким, тобто здатним легко адаптуватися до різних ситуацій;
7) наполегливим, тобто спрямованим на досягнення поставлених цілей;
8) логічним, тобто здатним своєчасно робити висновки на основі логічних міркувань і аналізу;
9) впевненим в собі, тобто здатним діяти незалежно, при цьому результативно взаємодіючи з іншими;
10) принциповим, тобто здатним діяти відповідально і в рамках етики, навіть якщо ці дії не завжди можуть викликати схвалення й іноді вести до незгоди або конфронтації;
11) готовим до вдосконалення, тобто мати бажання здобувати науку з різного роду ситуацій;
12) ввічливим до культурних особливостей, тобто хто виконує і поважає культурні традиції аудиту;
13) налаштованим на співпрацю, тобто результативно взаємодіє з іншими, в тому числі членами групи з аудиту і персоналом об'єкта аудиту. [21]

Знання та навички

Згідно ISO/IEC 27007 аудитори повинні володіти:

1) знаннями і навичками, необхідними для досягнення запланованих результатів аудитів;
2) загальними знаннями і навичками, пов'язаними з видом системи менеджменту, що перевіряється, а також знаннями і навичками, що відносяться до конкретної галузі.

Керівники груп з аудиту повинні мати додаткові знання і навички, необхідні для забезпечення керівництва групою з аудиту.

Загальні знання та навички аудиторів систем управління

Згідно ISO/IEC 27007 аудитори повинні володіти знаннями та навичками в областях, зазначених нижче.

а) Принципи, процеси і методи аудиту: знання і навички в цій області дозволяють аудитору забезпечити послідовне і системне проведення аудиту.

Аудитор повинен:

1) розуміти характер ризиків і можливостей, пов'язаних з аудитом, і принципи ризик-орієнтованого підходу до аудиту;
2) результативно планувати і організовувати роботу;
3) проводити аудит в рамках узгодженого графіка;
4) розставляти пріоритети і фокусуватися на питаннях, що мають важливе значення;
5) результативно обмінюватися інформацією в усній і письмовій формі (особисто або через перекладачів);
6) збирати інформацію шляхом результативного інтерв'ювання, вислуховування, спостереження і аналізу документованої інформації, включаючи записи та дані;
7) розуміти придатність і наслідки використання методів вибірки для аудиту;
8) сприймати і враховувати думки експертів;
9) проводити аудит процесу від початку до кінця, включаючи взаємозв'язку з іншими процесами і різними функціями, де це потрібно;
10) перевіряти актуальність і точність зібраної інформації;
11) підтверджувати достатність і придатність доказів аудиту для обґрунтування висновків і висновків аудиту;
12) оцінювати ті чинники, які можуть вплинути на достовірність висновків і висновків аудиту;
13) документувати заходи щодо аудиту та висновки аудиту, а також формувати звіти;
14) дотримуватися конфіденційності і заходів захисту інформації.

б) Стандарти для систем менеджменту і інші довідкові документи: знання і навички в цій області дозволяють аудитору розуміти область аудиту і застосовувати критерії аудиту, і повинні включати в себе наступне:

1) стандарти для систем менеджменту або інші нормативні або керівні / допоміжні документи, які використовуються для встановлення критеріїв і методів аудиту;
2) застосування стандартів для систем менеджменту перевіряється і іншими організаціями;
3) відносини і взаємодії між процесами системи (систем) менеджменту;
4) розуміння значущості та пріоритетності в рамках комплексу стандартів або довідкових документів;
5) застосування стандартів або довідкових документів в різних ситуаціях аудиту.

в) Організація і її контекст: знання і навички в цій області дозволяють аудитору зрозуміти структуру, цілі та методи управління аудиту і повинні включати в себе наступне:

1) потреби і очікування відповідних зацікавлених сторін, які впливають на систему менеджменту;
2) тип організації, побудова управління, розмір, структуру, функції і зв'язку;
3) загальний підхід до бізнесу і управління, процеси і відповідну термінологію, в тому числі планування, бюджетування та управління людьми;
4) культурні та соціальні аспекти аудиту.

г) Відповідні законодавчі, нормативні та інші вимоги: знання та навички в цій області дозволяють аудитору бути обізнаним про вимоги до організації і працювати в рамках цих вимог. Знання та навички, характерні для юрисдикції або діяльності об'єкта аудиту, процесів, продуктів і послуг, повинні включати в себе наступне:

1) законодавчі та нормативні вимоги і встановлюють їх держустанови;

2) основну юридичну термінологію;
3) порядок укладення договорів і контрактні зобов'язання. [21]

Загальна компетентність керівника групи з аудиту

Згідно ISO/IEC 27007 з метою сприяння результативному та ефективному проведенню аудиту керівник групи з аудиту повинен володіти компетентністю для:

1) планування аудиту та призначення завдань з аудиту відповідно до наявної компетентністю конкретних членів групи з аудиту;
2) обговорення стратегічних питань з вищим керівництвом об'єкта аудиту з метою визначити, враховувало воно опікується цими питаннями при оцінці ризиків і можливостей;
3) встановлення і підтримання конструктивних робочих відносин між членами групи з аудиту;
4) управління процесом аудиту, в тому числі:
   - результативного використання ресурсів в ході аудиту;
   - управління невизначеністю в досягненні цілей аудиту;
   - охорони здоров'я і безпеки членів групи з аудиту в ході аудиту, включаючи забезпечення дотримання аудиторами відповідних угод, що стосуються питань забезпечення здоров'я та безпеки;
   - керівництва членами команди з аудиту;
   - керівництва і консультування аудиторів-стажерів;
   - запобігання і врегулювання конфліктів і проблем, які можуть виникати в ході аудиту, включаючи, якщо необхідно, і ті, що виникають у групі з аудиту.
5) керівництва групою з аудиту з метою формування висновків з аудиту;
6) підготовки і остаточного формування звіту по аудиту. [21]

Коли аудит проводиться для кількох систем, член групи з аудиту повинен мати уявлення про взаємодію і синергії між різними системами менеджменту.

Керівники груп з аудиту повинні розуміти вимоги кожного зі стандартів систем менеджменту і усвідомлювати обмеженість своєї компетентності в кожному з видів систем менеджменту.

Забезпечення компетентності аудитора

Згідно ISO/IEC 27007 аудитор може отримати належну компетентність, використовуючи комбінації наступного:

1) успішне завершення навчальних програм, які охоплюють загальні знання і навички аудитора;
2) досвід роботи на відповідних технічних, управлінських або професійних посадах, пов'язаних з формуванням суджень, прийняттям рішень, вирішенням проблем та спілкуванням з керівниками, фахівцями, колегами, замовниками та іншими відповідними зацікавленими сторонами;
3) освіта або навчання і досвід в конкретній системі менеджменту і галузі, які розширюють загальну компетентність;
4) досвід аудиту, отриманий під керівництвом аудитора, компетентного в цій галузі. [21]

4.2 Критерії та методи оцінювання аудиторів СУІБ

Критерії повинні мати якісний характер (наприклад, демонстровані бажані особисті якості, знання або реалізація навичок при навчанні або на робочому місці) і кількісний (наприклад, досвід роботи і тривалість навчання в роках, кількість проведених аудитів, кількість годин підготовки в сфері аудиту).

Оцінка повинна проводитися з використанням двох або більше методів, зазначених у таблиці 4.2. При використанні таблиці 4.2 слід мати на увазі наступне:

1) описані методи являють собою набір можливостей і не стосуються в деяких ситуаціях;
2) різні методи з представлених можуть відрізнятися по своїй надійності;

3) для забезпечення об'єктивного, несуперечливого, неупередженого і надійного результату слід використовувати комбінацію методів. [21]

Таблиця 4.2 – Методи оцінки аудиторів

Метод оцінки	Цілі	Приклади
Аналіз записів	Перевірити підготовку аудитора	Аналіз записів про освіту, підготовці, стаж, професійної кваліфікації та досвіду аудитів
Зворотний зв'язок	Отримати інформацію про те, як сприймається робота аудитора	Опитування, анкети, особисті рекомендації, відгуки, претензії, оцінка результатів роботи, експертна оцінка
Інтерв'ю	Оцінити бажані особисті якості та навички спілкування, підтвердити інформацію і перевірити знання, отримати додаткову інформацію	Особисті інтерв'ю
Спостереження	Оцінити бажані особисті якості і здатність застосовувати знання та навички	Рольові ігри, спостереження в ході аудиту, фактичну якість роботи
Тестування	Оцінити бажані особисті якості, знання, навички та їх застосування	Усні чи письмові іспити, психометричне тестування

Інформація, яка зібрана про аудитора повинна бути порівняна з критеріями. Якщо аудитор, участь якого передбачається в програмі аудиту, не відповідає критеріям, то слід провести додаткове навчання, дати можливість

отримати додатковий досвід роботи або аудиту, після чого слід виконати повторну оцінку.

4.3 Висновки до розділу 4

Для успішного проведення комплексного аудиту СУІБ необхідно запросити компетентного аудитора. В розділі було розглянуто вимоги, що встановлюються до компетентності аудитора, а також методи оцінки аудиторів. Вибір професійного та незалежного аудитора є досить важливим фактором при проведенні комплексного аудиту СУІБ. Це дозволить в повній мірі в короткий термін оцінити наявні недоліки компанії та надати рекомендації по усуненню цих недоліків. Аудитор повинен доречно розробити програму аудиту та оцінити всі ризики і ресурси для його проведення.

РОЗДІЛ 5. РОЗРОБКА ПРОГРАМИ ТА ЦІЛЕЙ АУДИТУ СУІБ

5.1 Управління програмою аудиту

Згідно ISO/IEC 27007 повинна бути розроблена програма аудиту, яка може включати в себе аудити, орієнтовані на один або кілька стандартів системи управління, що проводяться або окремо, або в комбінації (комбінований аудит).

Обсяг програми аудиту повинен залежати від розміру і характеру об'єкта аудиту, а також від характеру, функціонального призначення, складності, типу ризиків і можливостей і рівня зрілості систем управління, що підлягають перевірці.

Функціонування системи менеджменту може бути ще більш складним, коли більшість важливих функцій передаються на аутсорсинг і управляються під керівництвом інших організацій. Особливу увагу необхідно приділити тому, де приймаються найважливіші рішення і хто складає вище керівництво системи менеджменту.

У випадку декількох місць знаходження / майданчиків (наприклад, в різних країнах) або де важливі функції передаються на аутсорсинг і управляються під керівництвом іншої організації, особливу увагу слід приділяти розробці, плануванню і підтвердженню програми аудиту.

У випадку невеликих або менш складних організацій програма аудиту може бути масштабувати відповідним чином.

Щоб зрозуміти контекст аудиту, програма аудиту повинна враховувати:

1) мету організації;
2) відповідні зовнішні і внутрішні чинники;
3) потреби і очікування відповідних зацікавлених сторін;
4) вимоги до інформаційної безпеки та конфіденційності. [21]

Планування програм внутрішнього аудиту та, в деяких випадках, програм аудиту зовнішніх постачальників може бути виконано для досягнення і інших цілей організації.

Особа, що управляє програмою аудиту, повинна гарантувати, що забезпечується цілісність аудиту та не надається неправомірного впливу в ході аудиту.

Пріоритет при аудиті повинен бути відданий виділенню ресурсів і вибору методів для елементів системи менеджменту з більш високим рівнем ризику і більш низьким рівнем показників діяльності.

Для управління програмою аудиту повинні бути призначені компетентні особи.

Згідно ISO/IEC 27007 програма аудиту повинна включати інформацію і визначати ресурси, що дозволяють результативно і ефективно проводити аудит в зазначені терміни. Інформація повинна включати:

1) мету програми аудиту;
2) ризики та можливості, пов'язані з програмою аудиту, і дії по їх обробці;
3) область (обсяг, межі, місця) кожного аудиту в рамках програми аудиту;
4) графік (кількість / тривалість / частота) аудитів;
5) типи аудиту, наприклад, внутрішні чи зовнішні;
6) критерії аудиту;
7) методи аудиту, які будуть використовуватися;
8) критерії відбору членів групи з аудиту;
9) відповідну документовану інформацію. [21]

Деяка частина цієї інформації може бути недоступна до тих пір, поки не буде завершено більш докладне планування аудиту.

Здійснення програми аудиту має контролюватися і оцінюватися на постійній основі для забезпечення досягнення його цілей. Програма аудиту повинна переглядатися з метою виявлення потреб в змінах і потенційних можливостях для покращення.

5.2 Визначення цілей програми аудиту

Замовник аудиту повинен гарантувати, що цілі програми аудиту для управління плануванням і проведення аудитів встановлено, і повинен забезпечити результативне виконання програми аудиту. Цілі програми аудиту повинні бути узгоджені зі стратегією розвитку замовника аудиту, а також бути пов'язані з політикою і цілями системи менеджменту.

Згідно ISO/IEC 27007 цілі можуть встановлюватися з урахуванням наступного:

1) потреб і очікувань відповідних зацікавлених сторін, як зовнішніх, так і внутрішніх;
2) характеристик процесів і вимог до процесів, продуктів, послуг і проектів, а також будь-яких змін в них;
3) вимог до системи менеджменту;
4) необхідності в оцінці зовнішніх постачальників;
5) рівня функціонування об'єкта аудиту і рівня зрілості систем управління, що відображаються відповідними показниками діяльності (наприклад, KPI), статистикою невідповідностей або інцидентів, або претензій від зацікавлених сторін;
6) виявлених в аудиту ризиків і можливостей;
7) результатів попередніх аудитів. [21]

Приклади цілей програми аудиту включають в себе наступне:

1) виявлення можливості поліпшення системи менеджменту і її функціонування;
2) оцінка здатності аудиту визначати її контекст;
3) оцінка здатності аудиту визначати ризики та можливості, а також розробляти і здійснювати результативні заходи по їх обробці;
4) підтвердження виконання всіх відповідних вимог, тобто законодавчих і нормативних вимог, зобов'язань щодо дотримання, вимог в рамках сертифікації на відповідність стандарту на систему менеджменту;

5) отримання і підтримка впевненості у можливостях зовнішнього постачальника;
6) оцінка її постійної придатності, відповідність і результативність системи менеджменту аудиту;
7) оцінка узгодженості цілей системи менеджменту зі стратегічним напрямком розвитку організації. [21]

5.3 Визначення та оцінка ризиків і можливостей, пов'язаних з програмою аудиту

Існують різні ризики і можливості, пов'язані з контекстом аудиту, які можуть вплинути на програму аудиту і на досягнення поставлених в ній цілей. Особам, що керуються аудитом слід виявити і донести до аудиту ризики і можливості, що враховуються при розробці програми аудиту і вимог до ресурсів, з тим, щоб було вжито належних заходів.

Згідно ISO/IEC 27007 ризики можуть бути пов'язані з:

1) плануванням, наприклад, неправильним завданням відповідних цілей аудиту та визначенням обсягу, кількості, тривалості, місць проведення і графіка аудитів;
2) ресурсами, наприклад, з тим, що передбачено недостатньо часу, оснащеності і / або підготовки для розробки програми аудиту або проведення аудиту;
3) вибором групи з аудиту, наприклад, недостатністю загальної компетентності для результативного проведення аудитів;
4) комунікацією, наприклад, погано працюючими процесами / каналами внутрішнього / зовнішнього обміну інформацією;
5) реалізацією, наприклад, неналежною координацією в рамках програми аудиту або недостатньою увагою до питань інформаційної безпеки та конфіденційності;

6) управлінням документованою інформацією, наприклад, неправильним визначенням необхідної документованої інформації, необхідної аудиторам і відповідним зацікавленим сторонам, нездатністю відповідним чином зберігати записи аудиту, щоб продемонструвати результативність програми аудиту;
7) моніторингом, аналізом і поліпшенням програми аудиту, наприклад, незадовільним моніторингом результатів програми аудиту;
8) доступністю і готовністю до співпраці аудиту і доступністю свідоцтв, які повинні бути зібрані. [21]

Можливості можуть включати в себе:

1) можливість проведення декількох аудитів за один раз;
2) мінімізацію часу і відстані при переїзді з одного місця на інше;
3) відповідність рівня компетентності групи з аудиту рівнем компетентності, необхідного для досягнення цілей аудиту;
4) узгодження дат проведення аудиту з доступністю ключових співробітників аудиту.

5.4 Розробка програми аудиту

5.4.1 Ролі та обов'язки осіб, що управляють програмою аудиту

Особа, що управляє програмою аудиту, повинна:

1) встановити обсяг програми аудиту, відповідний значимим цілям і будь-яким відомим обмеженням;
2) визначити зовнішні та внутрішні фактори, а також ризики і можливості, які можуть вплинути на програму аудиту, здійснити заходи по їх обробці;
3) забезпечити формування групи з аудиту і загальну компетентність в рамках заходів з аудиту, призначивши ролі, обов'язки і повноваження, а також дотримуючись принципу лідерства, наскільки це може бути застосовано;

4) розробити всі істотні процеси, включаючи процеси для:
   - координації та формування графіку всіх аудитів в рамках програми аудиту;
   - встановлення цілей аудиту, області і критеріїв аудитів, визначення методів аудиту та формування групи з аудиту;
   - оцінки аудиторів;
   - розробки процесів внутрішніх і зовнішніх комунікацій, в залежності від ситуації;
   - вирішення суперечок і обробки претензій;
   - наступних після аудиту дій, якщо це може бути застосовано;
   - звітності замовнику аудиту і відповідним зацікавленим сторонам, при необхідності.
5) визначити і гарантувати забезпечення всіма необхідними ресурсами;
6) гарантувати, що відповідна документована інформація підготовлена ;
7) здійснювати моніторинг, аналіз і поліпшення програми аудиту;
8) передавати програму аудиту замовнику аудиту і, при необхідності, відповідним зацікавленим сторонам. [21]

Особі, що управляє програмою аудиту, варто запитати у замовника аудиту схвалення програми аудиту.

5.4.2 Визначення обсягу програми аудиту

Особа, що управляє програмою аудиту, має визначити обсяг програми аудиту. Він може варіюватися в залежності від інформації, наданою об'єктом аудиту щодо її контексту.

У деяких випадках, в залежності від структури об'єкта аудиту або її діяльності, програма аудиту може складатися тільки з одного аудиту (наприклад, невеликий проект або організація).

Інші фактори, що впливають на обсяг програми аудиту, можуть включати в себе наступне:

1) мета, область і тривалість кожного аудиту і кількість аудитів, які повинні бути проведені, способи звітності і, у разі необхідності, подальші дії;
2) стандарти для систем менеджменту або інші застосовні критерії;
3) кількість, важливість, складність, ступінь подібності та місця виконання видів діяльності, що підлягають аудиту;
4) фактори, що впливають на результативність системи управління;
5) застосовні критерії аудиту, такі як заплановані в рамках відповідних стандартів для систем менеджменту заходи, законодавчі, нормативні та інші вимоги, виконувати які взяла на себе зобов'язання організація;
6) результати попередніх внутрішніх або зовнішніх аудитів, а також аналізу керівництва, наскільки це може бути застосовано;
7) результати аналізу раніше розроблених програм аудиту;
8) мова, питання культурної та соціальної сфери;
9) проблеми, які вказуються зацікавленими сторонами, такі як претензії споживачів, недотримання законодавчих, нормативних та інших вимог, виконувати які взяла на себе зобов'язання організація;
10) істотні зміни в контексті аудиту або її діяльності, а також відповідні ризики і можливості;
11) наявність інформаційно-комунікаційних технологій для підтримки заходів аудиту, зокрема, використання дистанційних методів аудиту;
12) наявність подій, що мали місце як всередині організації, так і за її межами, таких як невідповідності продуктів або послуг, витік інформації, нещасні випадки на виробництві, інциденти кримінального або екологічного характеру;
13) бізнес-ризики і можливості, включаючи заходи по їх обробці. [21]

5.4.3 Визначення ресурсів для виконання програми аудиту

Згідно ISO/IEC 27007 при визначенні ресурсів для програми аудиту, особі, що управляє аудитом, необхідно взяти до уваги:

1) фінансові та тимчасові ресурси, необхідні для розробки, виконання, управління і поліпшення заходів щодо аудиту;
2) методи аудиту;
3) наявність взагалі або конкретних аудиторів і технічних експертів, компетентність яких відповідає конкретним цілям програми аудиту;
4) обсяг програми аудиту, ризики та можливості, пов'язані з програмою аудиту;
5) час на проїзд і вартість, проживання та інші потреби, пов'язані з аудитом;
6) вплив різниці в часі.
7) наявність інформаційно-комунікаційних технологій (наприклад, технічних ресурсів, необхідних для проведення дистанційного аудиту з використанням технологій, що забезпечують віддалену спільну роботу);
8) наявність будь-якого необхідного інструментарію, технологій та обладнання;
9) наявність необхідної документованої інформації, визначеної на етапі розробки програми аудиту;
10) вимоги, пов'язані з умовами на об'єкті аудиту, включаючи будь-які допуски і оснащення (наприклад, перевірка анкетних даних, індивідуальні засоби захисту, вміння користуватися спеціальним одягом для дотримання режиму чистої кімнати). [21]

5.5 Виконання програми аудиту

Після розробки програми аудиту і визначення необхідних ресурсів потрібно здійснити оперативне планування і координацію всіх заходів в рамках цієї програми.

Згідно ISO/IEC 27007 особа, що управляє програмою аудиту, повинна:

1) довести до відома відповідних зацікавлених сторін інформацію про частини програми аудиту, включаючи пов'язані з нею ризики і можливості, і періодично інформувати їх про стан справ, використовуючи встановлені канали для внутрішніх і зовнішніх комунікацій;
2) визначити цілі, область і критерії кожного окремого аудиту;
3) вибрати методи аудиту;
4) координувати і визначати графік аудитів та інших заходів, що мають відношення до програми аудиту;
5) забезпечити необхідний рівень компетентності груп з аудиту;
6) забезпечити необхідні ресурси для груп з аудиту, як для окремих членів групи, так і в цілому для всієї групи;
7) забезпечити проведення аудитів відповідно до програми аудиту, управляючи всіма операційними ризиками, можливостями і проблемами (наприклад, несподіваними подіями) в міру їх виникнення в ході розгортання програми аудиту;
8) гарантувати, що відповідна документована інформація, пов'язана з заходами аудиту, належним чином управляється і підтримується;
9) визначити та впровадити робочі процедури, необхідні для моніторингу програми аудиту;
10) аналізувати програму аудиту з метою виявлення можливостей її поліпшення. [21]

5.5.1 Визначення цілей, області та критеріїв для конкретного аудиту

Для кожного окремого аудиту повинні бути встановлені цілі, область і критерії аудиту. Вони повинні відповідати загальним цілям програми аудиту.

Згідно ISO/IEC 27007 цілі аудиту можуть включати в себе наступне:

1) визначення ступеня відповідності перевіряється системи менеджменту або її частини критеріями аудиту;
2) оцінку здатності системи менеджменту сприяти організації дотримання відповідних законодавчих, нормативних та інших вимог, які організація зобов'язалася виконувати;
3) оцінку результативності системи менеджменту в досягненні очікуваних в її рамках результатів;
4) виявлення можливостей поліпшення системи менеджменту;
5) оцінку придатності та адекватності системи менеджменту з урахуванням контексту і стратегічного напрямку розвитку аудиту;
6) оцінку здатності системи менеджменту встановлювати і досягати цілі та результативно обробляти ризики і можливості в умовах мінливого контексту, включаючи здійснення відповідних заходів. [21]

Сфера аудиту повинна відповідати програмі і цілям аудиту. Вона включає в себе такі елементи, як місцезнаходження, функції, види діяльності і процеси, що підлягають аудиту, а також період часу, в який проводиться аудит.

Критерії аудиту використовують як еталон, за яким визначається відповідність. Вони можуть включати в себе один або декілька елементів з наступного переліку: застосовні політики, процеси, процедури, критерії результативності, в тому числі цілі, законодавчі та нормативні вимоги, вимоги системи менеджменту, інформація, пов'язана з контекстом, ризиками і можливостями, що встановлені об'єктом аудиту (включаючи вимоги відповідних зовнішніх / внутрішніх зацікавлених сторін), галузеві кодекси поведінки або інші заплановані заходи.

В випадку будь-яких змін в цілях, області або умовах аудиту програму аудиту слід відредагувати, якщо це необхідно, і передати зацікавленим сторонам для схвалення, якщо це необхідно.

Коли проводиться аудит по більш ніж одному напрямку менеджменту в один і той же час, важливо, щоб цілі, область і критерії аудиту були узгодженими в рамках відповідних програм аудиту по кожному напрямку. Деякі системи менеджменту можуть мати область аудиту, яка покриває всю організацію, а інші можуть мати область, яка зачіпає частину організації.

5.5.2 Вибір і визначення методів аудиту

Особа, що управляє програмою аудиту, має вибрати і визначити методи для результативного і ефективного проведення аудиту, в залежності від встановленої мети, області та критеріїв аудиту.

Аудити можуть проводитися на місці, віддалено або з поєднанням того і іншого. Застосування цих методів має бути належним чином збалансовано з урахуванням, крім усього іншого, пов'язаних ризиків і можливостей.

Якщо дві або більше аудиторських організації проводять спільний аудит однієї і тієї ж організації, особи, що керують різними програмами аудиту, повинні узгодити методи аудиту і розглянути наслідки з точки зору забезпечення ресурсами і планування аудиту. Якщо об'єкт аудиту застосовує дві або більше різних систем менеджменту, то в програму аудиту можуть бути включені комбіновані аудити. [21]

5.5.3 Вибір членів групи з аудиту

Особа, що управляє програмою аудиту, має призначити членів групи з аудиту, включаючи керівника групи і будь-яких технічних експертів, необхідних для конкретного аудиту.

Група з аудиту повинна бути сформована з урахуванням компетентності, необхідної для досягнення цілей конкретного аудиту в рамках встановленої області аудиту. Якщо є тільки один аудитор, він повинен виконувати всі відповідні обов'язки керівника групи з аудиту.

Щоб оцінити загальну компетентність групи з аудиту повинні бути виконані наступні кроки:

1) встановити необхідний рівень компетентності для досягнення цілей аудиту;
2) вибрати членів групи з аудиту таким чином, щоб група з аудиту володіла необхідною компетенцією.

Згідно ISO/IEC 27007 при визначенні розміру та складу групи з аудиту для конкретного аудиту необхідно звернути увагу на наступне:

1) загальна компетентність групи з аудиту, необхідна для досягнення цілей аудиту, з урахуванням області та критеріїв аудиту;
2) складність аудиту;
3) чи є аудит комбінованим або спільним;
4) обрані методи аудиту;
5) забезпечення об'єктивності і неупередженості, щоб уникнути будь-якого конфлікту інтересів в ході процесу аудиту;
6) здатність членів групи з аудиту результативно працювати і взаємодіяти з представниками об'єкта аудиту і відповідних зацікавлених сторін;
7) відповідні зовнішні / внутрішні чинники, такі як мова аудиту, а також соціальні та культурні особливості аудиту. Ці питання можуть бути вирішені або за рахунок власної компетентності аудитора, або за підтримки технічного експерта, а також необхідно враховувати потребу в перекладачах;
8) тип і складність процесів, що перевіряються. [21]

Якщо необхідно, то особа, що управляє програмою аудиту має проконсультуватися з керівником групи з питання формування групи з аудиту.

Якщо обрані в групу з аудиту аудитори не забезпечують необхідної компетентності, то в неї повинні бути включені технічні експерти з додатковою компетентністю.

Аудитори-стажери можуть бути включені в групу з аудиту, але повинні брати участь під керівництвом і наглядом аудитора.

Під час аудиту може знадобитися коригування складу групи з аудиту, наприклад, в разі виникнення конфлікту інтересів або проблем з компетентністю. Якщо виникає така ситуація, то її слід обговорити з відповідними сторонами (наприклад, керівником групи з аудиту, особами, що управляють програмою аудиту, замовником аудиту), перш ніж будуть зроблені будь-які зміни.

5.5.4 Призначення обов'язків керівника групи з аудиту для конкретного аудиту

Особа, що управляє програмою аудиту, повинна покласти обов'язки з проведення конкретного аудиту на керівника групи з аудиту.

Призначення має бути зроблено з достатнім запасом часу до наміченої дати проведення аудиту, щоб забезпечити належне планування аудиту.

Згідно ISO/IEC 27007 для результативного проведення конкретних аудитів керівнику групи з аудиту має бути надана така інформація:

1) мета аудиту;
2) критерії аудиту і будь-яка документована інформація, що має суттєве значення;
3) область аудиту, включаючи ідентифікаційні дані організації, її функції і процеси, що підлягають аудиту;
4) процеси аудиту і пов'язані з ними методи;
5) склад групи з аудиту;
6) контактні дані аудиту, місця знаходження, терміни і тривалість заходів щодо аудиту, які повинні бути проведені;

7) ресурси, необхідні для проведення аудиту;
8) інформація, необхідна для оцінки та прийняття заходів щодо виявлених ризиків і можливостей для досягнення цілей аудиту;
9) інформація, що необхідна керівнику групи з аудиту для забезпечення результативності програми аудиту. [21]

Згідно ISO/IEC 27007 інформація про призначення обов'язків повинна також включати наступне:

1) робоча мова аудиту та мову для звіту, якщо вони відрізняються від мови, яка використовується аудитором або об'єкт аудиту, або того й іншого;
2) необхідний вміст звіту про аудит і кому він повинен бути спрямований;
3) питання, що стосуються конфіденційності та інформаційної безпеки, як це вимагається програмою аудиту;
4) будь-які заходи охорони здоров'я, навколишнього середовища та безпеки щодо аудиторів;
5) вимоги, пов'язані з переїздами і доступам до віддалених місцях аудиту;
6) будь-які вимоги, пов'язані з секретністю і наданням прав доступу;
7) будь-які дії, які повинні бути враховані, наприклад, наступні дії, визначені за результатами попереднього аудиту;
8) координація з іншими заходами аудиту, наприклад, коли кілька різних груп проводять аудит схожих або пов'язаних процесів на різних майданчиках або в разі проведення спільного аудиту. [21]

Якщо проводиться спільний аудит, важливо досягти угоди між організаціями, які проводять аудити, до того, як аудит почнеться, по конкретним обов'язкам кожної зі сторін, зокрема, щодо повноважень керівника група з аудиту, призначеного для даного аудиту.

5.5.5 Управління результатами виконання програми аудиту

Згідно ISO/IEC 27007 особа, що управляє програмою аудиту, повинна гарантувати, що виконані наступні заходи:

1) проведена оцінка досягнення цілей кожного аудиту в рамках програми аудиту;
2) розглянуті і затверджені звіти про аудити з точки зору повноти охоплення області аудиту та досягнення цілей;
3) проведено аналіз результативності заходів, прийнятих за результатами аудиту;
4) звіт про результати аудиту розісланий відповідним зацікавленим сторонам;
5) визначено необхідність проведення додаткового аудиту.

Особа, яка управляє програмою аудиту, повинна враховувати, в залежності від обставин:

1) інформування частин організації, що не увійшли в область аудиту, про результати аудиту та кращі практики;
2) наслідки для інших процесів. [21]

5.5.6 Контроль протоколів за програмою аудиту

Особа, що управляє програмою аудиту, повинна гарантувати, що записи з аудиту створюються і управляються, щоб продемонструвати виконання програми аудиту. Повинні бути розроблені процеси, що гарантують, що будь-які потреби в інформаційній безпеці і конфіденційності, пов'язані з записами по аудиту, задовольняються. Записи можуть включати в себе наступне:

1) записи, пов'язані з програмою аудиту:
   - графік аудитів;
   - мета і обсяг програми аудиту;

- що визначають ризики і можливості в рамках програми аудиту, а також відповідні зовнішні і внутрішні чинники;
- результати аналізу результативності програми аудиту;

2) записи, що відносяться до конкретного аудиту:
   - плани аудиту і звіти з аудиту;
   - об'єктивні свідчення аудиту та висновки;
   - звіти про невідповідності;
   - звіти про корекції та коригувальні дії;
   - звіти про подальші дії;
3) записи, пов'язані з групою з аудиту, які стосуються таких питань:
   - компетентність і оцінка результативності членів групи з аудиту;
   - критерії для формування груп з аудиту і вибору членів групи;
   - підтримування та поліпшення компетентності. [21]

Форма і рівень деталізації записів повинні давати можливість продемонструвати, що цілі програми аудиту були досягнуті.

5.6 Моніторинг програми аудиту

Згідно ISO/IEC 27007 особа, що управляє програмою аудиту, повинна гарантувати оцінку:

1) того, що був витриманий графік і досягнуті цілі аудиту;
2) роботи членів групи з аудиту, в тому числі керівника групи з аудиту і технічних експертів;
3) здатності групи з аудиту виконувати план аудиту;
4) зворотного зв'язку від замовників аудиту оргінзації, аудиторів, технічних експертів та інших відповідних сторін;
5) достатності та адекватності документованої інформації щодо процесу аудиту в цілому. [21]

Деякі фактори можуть вказувати на необхідність внести зміни в програму аудиту. Вони можуть включати в себе зміни в:

1) висновках аудиту;
2) продемонстрованому рівні результативності та зрілості системи менеджменту;
3) результативності програми аудиту;
4) області аудиту і програми аудиту;
5) системі менеджменту аудиту;
6) стандартах та інших вимогах, які організація зобов'язалася виконувати;
7) зовнішніх постачальників;
8) виявлених конфліктах інтересів;
9) вимогах замовника аудиту. [21]

5.7 Перегляд і поліпшення програми аудиту

Особа, що управляє програмою аудиту, і замовник аудиту повинні аналізувати програму аудиту для оцінки того, чи були досягнуті її мета. Уроки, витягнуті з аналізу програми аудиту, слід використовувати в якості вихідних даних для постійного поліпшення програми.

Згідно ISO/IEC 27007 особа, що управляє програмою аудиту, повинна забезпечити наступне:

1) аналіз виконання програми аудиту в цілому;
2) виявлення областей і можливостей для поліпшення;
3) внесення змін до програми аудиту в разі потреби;
4) відстеження постійного професійного розвитку аудиторів;
5) надання звіту про результати виконання програми аудиту і спільного з замовником аудиту та відповідними зацікавленими сторонами аналізу.

При аналізі програми аудиту слід враховувати наступне:

1) результати і тенденції, виявлені під час моніторингу програми аудиту;

2) відповідність процесам програми аудиту і відповідної документованої інформації;

3) зростаючі потреби і очікування відповідних зацікавлених сторін;

4) записи за програмою аудиту;

5) альтернативні або нові методи аудиту;

6) альтернативні або нові методи оцінки аудиторів;

7) результативність заходів з обробки ризиків і можливостей, а також внутрішніх і зовнішніх факторів, пов'язаних з програмою аудиту;

8) конфіденційність і питання інформаційної безпеки, пов'язані з програмою аудиту.

5.8 Висновки з розділу 5

В розділі описані короткі рекомендації ISO/IEC 27007 для успішної розробки програми аудиту, визначення цілей та оцінки ризиків аудиту. Також важливим аспектом є аналіз наявних ресурсів, що дозволить правильно розділити аудит на етапи. Обов'язково повинен проводитись моніторинг програми аудиту та визначені рекомендації для поліпшення програми аудиту. По завершенню аудиту аудитор повинен представити звіт в якому буде задокументована інформація щодо процесу аудиту в цілому.

РОЗДІЛ 6. РОЗРАХУНОК ТРИВАЛОСТІ АУДИТУ СУІБ ТА ТОЧОК ПЕРЕХОДУ МІЖ ЕТАПАМИ

6.1 Розрахунок тривалості аудиту СУІБ

Досить важливим аспектом є правильність розрахунку тривалості аудиту та управління виділеними матеріальними ресурсами. Визначити тривалість аудиту можна наступним чином.

Нехай якість СУІБ характеризується рівнем ризиків

$$R = \sum_i N_i * p_i(N_i) \qquad (6.1.1)$$

пов'язаних з можливостями реалізації загроз безпеки щодо ресурсів ІБ, де

N_i – збиток, очікуваний при реалізації загрози;

$p_i(N_i)$ – ймовірність ризику ІБ.

Виразимо p_i через ймовірність запобігання ризику z_i:

$$p_i(N_i) = (1 - z_i(N_i)) \qquad (6.1.2)$$

Тоді вираз (6.1.1) перепишемо в наступному вигляді:

$$R = \sum_i N_i * (1 - z_i(N_i)) \qquad (6.1.3)$$

Нехай z_{ni} гранично досяжний на даному етапі вимірювань показник якості ІБ. Тоді приріст показника в результаті впровадження допрацювань і уточнення політик безпеки СУІБ після проведення етапу вимірів можна представити у вигляді

$$dz_i = \omega_i(z_{ni} - z_i)dt, \qquad (6.1.4)$$

де ω_i – середня інтенсивність змін, що вносяться до СУІБ після чергового етапу вимірювань.

Розділимо змінні з виразу (6.1.4):

$$\frac{dz_i}{z_{ni} - z_i} = \omega_i dt \qquad (6.1.5)$$

Тепер проінтегруємо вираз (6.1.5). Ліву частину в межах $[z_0, z_i]$, в праву в межах $[t_0, t_i]$:

$$\int_{z_0}^{z_i} \frac{dz_i}{z_{ni} - z_i} = \int_{t_0}^{t_i} \omega_i dt$$

Звідси отримаємо наступний результат:

$$\ln\frac{z_{ni}-z_i}{z_{ni}-z_{0i}} = -\omega_i(t_i - t_{0i}) \qquad (6.1.6)$$

Тепер з виразу (6.1.6) визначимо ймовірність запобігання ризику ІБ z_i:

$$z_i = z_{ni} - (z_{ni} - z_{0i})e^{-\omega_i(t_i - t_{0i})} = z_{ni} - (z_{ni} - z_{0i})e^{-\omega_i\tau_i}$$

Якщо правильно організувати систему вимірювань рівня ризиків ІБ по ходу допрацювання політик безпеки з кожним наступним етапом ймовірність запобігання ризику буде збільшуватись, а середня інтенсивність змін, що вносяться до СУІБ буде зменшуватись. Тому будуть справедливі наступні співвідношення:

$$z_{ni} > z_{ni-1},\ \omega_i < \omega_{i-1}$$

Тобто завдання складання плану вимірювань СУІБ можна сформулювати як пошук оптимального розподілу часу на етапах вимірювань.

Тоді, використовуючи вираз (6.1.6) отримаємо загальний час вимірювань, підсумовуючи тривалості кожного і-го етапу вимірювань

$$T = \sum_{i=1}^{k}\tau_i = \sum_{i=1}^{k}\frac{1}{\omega_i}\ln\frac{z_{ni}-z_{0i}}{z_{ni}-z_i} \qquad (6.1.7)$$

З наведених розрахунків робимо висновок, що тривалість вимірювань буде визначатися положенням точок переходу від одного етапу до іншого, тобто значеннями z_i, $i = 1, k$ - 1 ($z_{ik} > z_T$, z_T – необхідне значення). Тоді задача зводиться до знаходження значень показника z_i, що забезпечують мінімальний час проведення вимірювань за умови, що після k етапів забезпечується досягнення необхідного рівня показника z_T.

6.2 Знаходження точок переходу між етапами

Скористаємось принципом динамічного програмування (принципом оптимальності), що означає оптимізацію від кінцевої точки. Тоді для довільного кроку тривалість аудита буде визначатись як:

$$T = \tau_k + \tau_{k-1} + \tau_{k-2} + \cdots + \tau_i$$

На першому етапі $T_k = \tau_k$.

На другому етапі $T_{k-1} = \tau_k + \tau_{k-1}$.

Використовуючи вираз (6.1.7) отримуємо:

$$T_{k-1} = \frac{1}{\omega_k}\ln\frac{z_{nk}-z_{0k}}{z_{nk}-z_T} + \frac{1}{\omega_{k-1}}\ln\frac{z_{nk-1}-z_{0k-1}}{z_{nk-1}-z_{0k}} \qquad (6.2.1)$$

Умову оптимального переходу від *k*-го етапу до *(k-1)* етапу можна отримати, продиференціювавши складові T_{k-1} з виразу (6.2.1). Після обчислення прирівняємо результати:

$$\omega_k(z_{nk} - z_{0k}) = \omega_{k-1}(z_{nk-1} - z_{0k}) \quad (6.2.2)$$

Отже, оптимальному моменту переходу від k-го етапу до *(k-1)* етапу вимірів відповідає точка рівності швидкостей зміни показника z на *(k-1)* і *k*-му етапах.

Тобто для виразу (6.2.2) це точка z_{0k}. Знайдемо її. Спочатку розкриємо дужки:

$$\omega_k z_{nk} - \omega_k z_{0k} = \omega_{k-1} z_{nk-1} - \omega_{k-1} z_{0k}$$

Перенесемо змінну z_{0k} в одну сторону, все інше в другу:

$$\omega_{k-1} z_{0k} - \omega_k z_{0k} = \omega_{k-1} z_{nk-1} - \omega_k z_{nk}$$

Звідси виразимо z_{0k}:

$$z_{0k} = \frac{\omega_{k-1} z_{nk-1} - \omega_k z_{nk}}{\omega_{k-1} - \omega_k} \quad (6.2.3)$$

Тобто z_{0k} й буде оптимальним рівнем показника якості, при якому потрібно перейти з одного етапу на інший.

Розглянемо приклад. Вимірювання були розбиті на чотири етапи. Необхідний рівень показника якості СУІБ – ймовірності запобігання несанкціонованому доступу до мережевої інфраструктури організації заданий значенням $z_T > 0{,}95$, а початковий рівень показника якості $z_0 = 0{,}5$. В ході виконання етапів вимірювань, вводилися удосконалення в засоби контролю і управління СУІБ.

Наприклад, значення показників якості та інтенсивності змін наведені в таблиці 6.2:

Таблиця 6.2 – Значення показників якості та інтенсивності змін

k	1	2	3	4	5
z_k	0,8	0,85	0,9	0,94	0,97
ω_k	0,04	0,035	0,03	0,02	0,01

За допомогою виразу (6.2.3) знайдемо оптимальні точки переходу від одного етапу до іншого. Для обрахунків використаємо мову програмування Python та модуль matplotlib для побудови графіку (рисунок 6.2). Код програми наведений в додатку А.

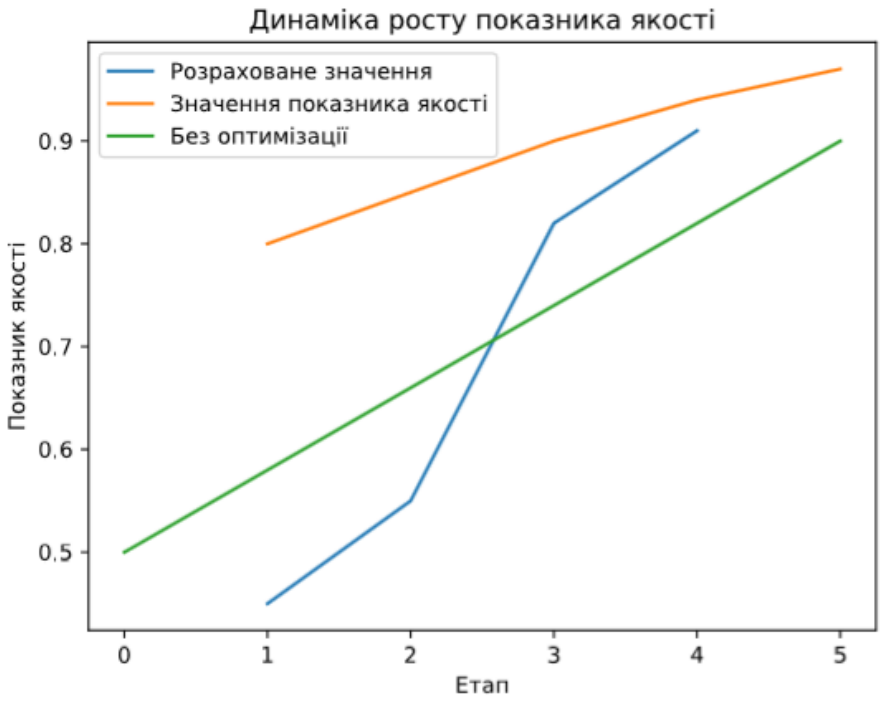

Рисунок 6.2 Динаміка росту показника якості

Після рішення задачі оптимізації розподілу часу по проведеним заходам (таблиця 5) отримані значення точок переходу від одного етапу вимірювань до іншого. Згідно з отриманими даними зростання показника якості після оптимізації максимальний, до початку 4 етапу вимірювань досягнутий рівень z_4 = 0,9. При цьому динаміка росту показника якості без оптимізації досягнула б цього рівня тільки до початку 5 етапу. Як бачимо, потрібний рівень може бути досягнутий за менший час.

6.3 Висновки до розділу 6

Запропонована методика дозволяє на основі моделі динаміки показника якості СУІБ здійснювати планування розподілу тимчасових або матеріальних ресурсів за етапами вимірювань. Особливістю даного підходу є використання не тільки апріорних, але і апостеріорних даних при початковому плануванні вимірювань, а також для коригування плану після кожного вимірювання. Це дозволяє оптимізувати використання ресурсу призначеного для вимірювань відповідно до обраних критеріїв.

ВИСНОВКИ

Для того щоб оцінити реальний стан захищеності ресурсів інформаційно-комунікаційних систем (ІТС) та їх здатність протистояти зовнішнім і внутрішнім загрозам безпеці, необхідно регулярно проводити аудит інформаційної безпеки.

Мета проведення аудиту інформаційної безпеки – оцінка стану безпеки ІТС та розробка рекомендацій щодо застосування комплексу організаційних заходів та програмно - технічних засобів, спрямованих на забезпечення захисту інформаційних та інших ресурсів ІТС від загроз інформаційній безпеці.

В ході аудиту інформаційної безпеки одним з завдань, які вирішуються, є аудит СУІБ.

Сучасні реалії проектування та побудови систем забезпечення інформаційної безпеки (СЗІБ) вимагають орієнтацію на міжнародні стандарти та рекомендації.

Аудит інформаційної безпеки в сучасних умовах є одним з найбільш ефективних інструментів отримання незалежної і об'єктивної оцінки поточного рівня захищеності будь-якого економічного суб'єкта як від існуючих, так і потенціальних загроз. Результати аудиту інформаційної безпеки дозволяють сформувати стратегічні установки розвитку, що відповідають сучасним викликам системи забезпечення інформаційної безпеки для вказаного суб'єкта. Однак слід розуміти, що застосування на практиці аудиту інформаційної безпеки має бути не епізодичним, а регулярним, що дозволяє не тільки виявити вже доконаний факт, а й передбачити потенційні загрози.

Для досягнення поставленої мети в роботі вирішені наступні задачі:

1) визначення місця аудиту СУІБ в системі забезпечення інформаційної безпеки;
2) аналіз стандартів щодо здійснення аудитів СУІБ та принципів проведення аудиту СУІБ;

3) дослідження питань оцінювання аудиторів СУІБ та їх компетентності для задоволення потреб програми аудиту СУІБ;
4) дослідження основних принципів розробки програми та цілей аудиту СУІБ;
5) аналіз провідних вказівок щодо управління програмою аудиту;
6) розрахунок тривалості аудиту СУІБ та оптимальних точок переходу між етапами аудиту.

Таким чином, в роботі розроблено комплекс питань щодо аудиту СУІБ, які в сукупності і складають Методику проведення комплексного аудиту СУІБ для захисту інформаційних активів організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27007:2017 / Information technology – Security techniques – Guidelines for information security management systems auditing. // – 2013. – 41 с.

2. Цвілій О.О. Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою / Науковий журнал «Телекомунікаційні та інформаційні технології». – 2014. – № 2. – с. 73-79.

3. Цвілій О.О. Системи управління інформаційною безпекою: гармонізація з міжнародними стандартами, правилами та процедурами. / Перша всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації». Збірник тез. – 2015. – с. 107-11.

4. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України від 9 січня 2007 року № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – с. 102.

5. Овсянніков В.В., Дехтяр С.В., Паламарчук С.А., Черниш Ю.О., Шемендюк О.В. Аналіз нормативно-правових та організаційнотехнічних аспектів забезпечення інформаційної безпеки. / Modern Information Technologies in the Sphere of Security and Defence № 3(24). – 2015. – 7 с.

6. Безпека інформаційних систем [Електронний ресурс] – Режим доступу ресурсу: https://pidruchniki.com/74227/informatika/bezpeka_informatsiynih_sistem

7. ISACA, Rolling Meadows. COBIT 5: Бизнес-модель по руководству и управлению ИТ на предприятии. – 2012. – 94 с.

8. Van Haren Publishing. The ITIL® Process Manual Key Processes and their Application. – 2012. – 55 с.

9. Иванова Н. Почему IT-компаниям необходим сертификат ISO/IEC 27001? [Електронний ресурс] – Режим доступу ресурсу: https://easy-standart.by/IT-post.html

10. Суханов А.В., Смирнов А.С., Хитов С.Б. Управление информационной безопасностью предприятий оборонно-промышленного комплекса в контексте стандарта ISO 27001:2013. – 2016. – 16 с.

11. Hinson G. The ISO27k Standards. – 2018. – 7 с.

12. ISO/IEC 27000:2018 / Information technology – Security techniques – Information security management systems – Overview and vocabulary. // – 2018. – 27 с.

13. ISO/IEC 27001:2013 / Information technology – Security techniques – Information security management systems – Requirements. // – 2013. – 23 с.

14. ISO/IEC 27006:2015 / Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems // – 2015. – 35 с.

15. ISO/IEC 27002:2013 / Information technology – Security techniques – Code of practice for information security management. // – 2013.

16. ISO/IEC 27003:2017 / Information technology – Security techniques – Information security management systems – Guidance // – 2017. – 45 с.

17. ISO/IEC 27004:2016 / Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation. // – 2016. – 58 с.

18. ISO/IEC 27005:2018 / Information technology – Security techniques – Information security risk management. // – 2018. – 56 с.

19. ISO/IEC 27011:2016 / Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations. // – 2016. – 31 с.

20. Ситнов А. А., Уринцов А. И. Аудит информационных систем: монография для магистров. М.:Юнити-Дана – 2014. – 239 с.

21. Ситнов А. А. Организация аудита информационной безопасности. – 2016. – 9 с.

22. ISO 19011:2018 Руководящие указания по аудиту систем менеджмента /перекл. А. Горбунова./ – 2018. – 58 с.

ДОДАТОК А

Код програми на мові програмування Python

```
import matplotlib.pyplot as plt
plt.switch_backend('agg')

z = [0.8, 0.85, 0.9, 0.94, 0.97]
w = [0.04, 0.035, 0.03, 0.02, 0.01]
no_opt = [0.5, 0.9]

opt_etaps = range(1, 5)
z_etaps = range(1, 6)
no_opt_etaps = [0, 5]


def histogram(number_list):
    plt.xlabel('Етап')
    plt.ylabel('Показник якості')
    plt.title('Динаміка росту показника якості')
    plt.plot(opt_etaps, number_list, label='Розраховане значення')
    plt.plot(z_etaps, z, label='Значення показника якості')
    plt.plot(no_opt_etaps, no_opt, label='Без оптимізації')
    plt.legend()
    plt.savefig('practice.pdf')

zopt_list = []

for k in range(0, 4):
    formula_opt = (w[k]*z[k] - w[k+1]*z[k+1])/(w[k] - w[k+1])
    zopt_list.append(round(formula_opt, 2))

histogram(zopt_list)
```